Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against Hackers

Hector Cruz Platon

Department of Doctoral Studies, Colorado Technical University

Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against Hackers

A Dissertation Presented in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Computer Science

by

Hector Cruz Platon

Department of Doctoral Studies, Colorado Technical University

December 2022

Committee Members Kelly

Hughes, D.C.S.,Chair

Jeffrey Butler, Ph.D., Committee Member

Abdullah Alshboul, D.B.A., CommitteeMember

DocuSign Envelope ID: B5B72E6E-A9E3-4924-9634-C8B56A3633A9

Signature Page

Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against Hackers

Hector Cruz Platon

Approved by Doctoral Committee:

DocuSigned by:
kelly Hughes, DCS
[illegible]

December 20, 2022

DissertationChair Date

DocuSigned by:
Abdullah Alshboul, DBA
[illegible]

December 20, 2022

CommitteeMember Date

DocuSigned by:
Jeffrey Butler, Ph.D.
3C8D88D6CCD146C...

December 20, 2022

Committee Member Date

Colorado Technical University®

Abstract

The transportation and automotive industry have seen the shifts and effects of innovation within the last decade, from the addition of critical messaging technologies, event response systems, to safety integration of each user initiated by safety messaging systems to almost all private utility vehicles to a public utility vehicle, all have seen either responsive or unresponsive layers of usability and functionality issues, together with the need for safety and protection of each users and riders. These assistive technologies are supposed to help drivers and operators in their daily driving routine, believed to be connected to a myriad of networked hardware and software, and arguably to be either be cost effective or safety limited. The study exploring vehicle security improvement framework in the safety messaging system to protect against hackers delivered responses from 6 subject matter experts within the public transit authority, cloud supply chain companies, and network providers that have invested greatly in vehicle ad hoc network technologies. Thematic analysis was chosen as a qualitative method design to extract themes from the critical answers through the semi-structured interview retrieved from general responses from the subject matter experts. The general findings were extracted from the major themes 1 through 5. The general findings are the following (1) Automotive Organizations and Transit Authority Leaders have to Manage Vehicle Cyber Risks Throughout the Vehicle Lifecycle, (2) Automotive Organization and Transit Authority Should Be Involved in Engineering a Secure Vehicle by Design, (3) Engineering Vendor Teams Should Detect and Respond to Major Incidents within the Vehicle Lifecycle.

Keywords: safety messaging system, event response systems, safety integration, vehicle ad hoc networks, vehicle security improvement framework, automotive informatics security.

Acknowledgments

I wish to express my heartfelt gratitude to my mom Mutya, and dad Ramon, for their undying support throughout my education who if alive today would be my first cheer leaders. Dad you have seen my struggles at the beginning of the writing, but you knew I had a talent and could frame the thesis and should keep doing it. To my sisters Maria Isabel and Francine, you have seen the dedication placed into putting up the chapters together and thank you for your time and assistance with taking a second look.

To my dear wife, Kays, thank you for believing that this dissertation project can be done even though there have been many life event's lumped into finishing the dissertation from our wedding, to your pregnancy, to the birth of Keira Ysobel, to the tireless nights we had to share taking care of Keira while doing the third chapter, fourth, and fifth chapter was all being written. To my dear baby Keira Ysobel, know that you are the future and no matter what youdo in life, I will support you.

I want to extend my gratitude to my research supervisor and dissertation director Dr.

Kelly Hughes for her never ending commitment to excellence, guidance, and approach in getting a qualifiable dissertation submitted. This is for you, too. I want to also thank Dr. Steve Munkeby for helping me formulate chapter headings, completing a TRIO process, and formulating the conceptual framework. I wish to express gratitude to Dr. James Webb for seeing through my literature review. Also, I want to extend my thank you's to Dr. Jeffrey Butler and Dr. Abdullah Alshboul for their assistance, commitment to guidance, proofreading the tables and charts, and intelligent remarks to connect all statements. Again, thank you for everything.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

As passengers and motorists, the goal was to reach our destination in safety. With the advent of multi-connected core and extended systems connected with our in-vehicular multi-functional units, primarily that affects the safety messaging systems, drivers are pressed to be more cautious in our rides due to ineffectual and undesirable system security performance,and automobile maker's misleading representation of the automotive security posture. According to Researcher Alexander Much (2016), of Software Quality Professional, Systems and software engineering for vehicles have become rather more complex, in line with the complexity of the systems that are built today. The advent of the connected car, which has enlarged the attack surface significantly and made it possible to attack multiple vehicles or even a whole fleet remotely (Much, 2016).

Secondly, a recent example of a security issue that has been publicly recognized is the "Connected Drive" system by BMW. It was possible, for example, to remotely unlock the doors of the car (Spaar, 2015). BMW was able to update and secure its systems over the air. Another example of a similar fleet-wide attack was targeted at the Nissan Leaf. Researcher and Penetration Tester Troy Hunt (Hunt, 2016) was able to use remote features sniff behavioral data from end users such as reading data about individual trips, travel distances, or turning on the air conditioner. The attack was very simple; all Hunt had to do was type a specially formatted URL into a standard web browser. Consequently, the remote functionality had to be taken offline (Spaar, 2015; Hunt, 2016).

Lastly, another prominent attack, due to media coverage and its safety relevance, were performed by researcher and penetration tester Miller and Vlasek on Chrysler / Jeep model (Miller & Valasek, 2015). Much of the desire and demand to perform the test publicly was showcase how in-vehicular systems can be easily be manipulated. Also, the showcasing how bad the requirement and inability of automakers to see the need for securing its complex application systems, now more troubling than ever safety messaging systems, affecting motorists and passengers by default, with external threats on the rise, and security posture in question to the public motorist and end user.

Study Problem/Opportunity

There had been vulnerabilities in the vehicles safety messaging system which were exposed to external hackers. The research found out that the generation of multi-functional units (Yoo et al*.,* 2012), next-generation interface, (Stocklein et al*.,* 2009) and connected cars provide motorists a wealth of system and vehicular hardware information, vehicular performance, and personalized vehicular content selection that is made vulnerable due to undeniable security exposures to threats and attacks, primarily through safety messaging system units (Yoo et al., 2012; Stocklein et al., 2009). Within this segment, registered motorists store, modify, and change their preference settings inside the cabin, with ease of access, also underwhelming the system with an enlarged attack surface which may affect the integrity of multi-functional units, or in-vehicular systems.

These privacy-sensitive data (Nawrath et al., 2016) attracted attackers and hackers at large from significant manufacturer embedded backdoors (Tien et al., 2018), infiltrated (Krall et al., 2016), penetrated (Patel et al., 2019), and assumed guidance of vehicular operations, making safety messaging system insecure (Nawrath et al., 2016; Tien et al., 2018; Krall et al., 2016; Patel et al., 2019). Insecurity among in-vehicular units was a multi-jurisdiction problem and lately had become a systemic problem for the automotive manufacturing organizations operating in an information-centric, data-driven, and security-aware environment. As automotive manufacturers, embedded systems, third-party data providers, architectural security engineering, and data custodial partners marched to safeguard the overall confidentiality, integrity, and availability of information in our vehicle, it was important to acknowledge and examine the state of security, security posture-at-large, within these in-vehicular applications as we partaken in the fight for a more secure, safe, and protected system, to alleviate and recompense for security risks that may harm passengers (Amin et al., 2015).

Study Purpose

The purpose of the proposed qualitative study was to explore the vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers. The research participant consisted of at least 6 subject matter experts as participant respondents who were qualified and expressed interest in the study as participant respondents. These remaining participant respondents expressed interest and came from various backgrounds of network operations, cybersecurity operations management, federal cybersecurity contracting, transit authority organizations that work within the automotive sector, who was available at the time of the research and were distributed into study subgroups.The research respondents were qualified within the automotive informatics security research semi-structured interviews consistently came from: (a) automotive (network or security) system providers (Oh et al., 2005), (b) automotive organizations (McHugh, 1998), (c) cloud service providers (Kang et al., 2014), and (d) the vehicular participants (Kim et al., 2019) as they promote the formulation of safety and standards for safety messaging systems (Oh et al., 2005; McHugh, 1998; Kang et al., 2014; Kim et al.,2019).

The research exposed improvement framework aspects from specific problems that might arise within various vehicular ad hoc network (VANETs) technologies, particularly the safety messaging system, with its association with automotive informatics security, built through integration and execution, as they would affect many integral systems and platforms such that may affect the graphical user interface representation of passenger data, from *Car-to-Car* (Widhiasi et al., 2010), *Car-to-Cloud* (Pillman et al*.,* 2017), to *Car-to-Infrastructure* (Meuleners et al., 2014) information that affects *data-in-transit* (DiT) and *data-at-rest* (DaR) standards (Coventry, 2015), security limitations of devices (*car-to-car*) that involves transmitter signals, to derailing vehicles autopilot presence, and user data integrity for in-motion users (Widhiasi et al., 2010; Pillman et al., 2017; Meuleners et al., 2014; Coventry, 2015).

Lastly, since most car manufacturers were not too far away with standardizing smart car technologies that enabled the *Internet of Vehicles* (IoV) to make vehicles more interactive with humans, vehicular devices, and infrastructure as seamlessly as possible and lately as it begun to be associated with newer automotive production lines. Lastly, there would be a basic need to safeguard passengers, vulnerable road users (VRUs), and drivers from the vulnerable components and limitations of newer trending technologies within the in-car systems (Butler, 2016) that surface and interact with safety messaging systems.

Research Question

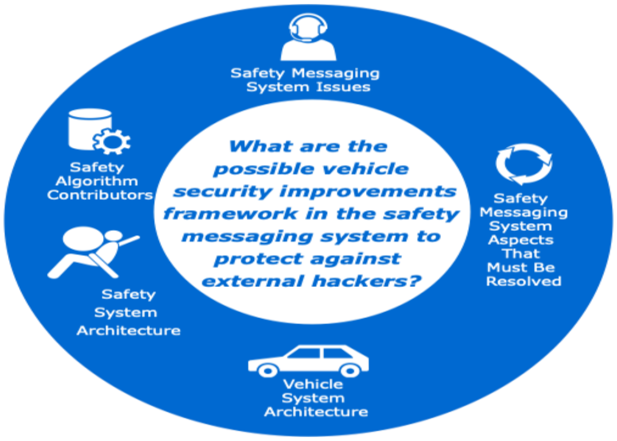
Q1

What are the possible vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers?

Conceptual Framework

Figure 1 *Conceptual Framework of the Possible Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers*

What are the possible vehicle security improvement framework in the safety messaging system to protect against external hackers?


Safety Messaging System Issues
Safety Algorithm Contributors
What are the possible vehicle security improvements framework in the safety messaging system to protect against external hackers?
Safety Messaging System Aspects That Must Be Resolved
Safety System Architecture
Vehicle System Architecture

Note. Conceptual framework is compounded to have been designed by multiple IoV researchers. Vehicle System Architecture, by Seigel, Erb, & Sarma, 2018. Safety System Architecture, by Ghafoor, Kong, Zeadally, Sadiq, Epiphaniou, Hammoudeeh, Bashir, and Mumtax, 2020. Safety Algorithm Contributors, by Kang and Kang, 2016. Safety Messaging

System Issues, by Petit and Mammeri, 2013. Safety Messaging System Aspects That Must Be Resolved, by Jackson, 2020.

The scope of the framework consisted of at least four to five parts: (1) vehicular system architecture, (2) safety system architecture, (3) safety algorithm contributors, (4) safety messaging system issues, and (5) safety messaging system aspects that must be resolved, as seen on Figure 1, to perpetuate the exploration of automotive vehicle improvements of system architects to reduce the susceptibility of the safety messaging system to external hackers. The attributes to safety and further improvements were examined against stakeholder's practical knowledge, skills, and abilities (KSA) with using safety messaging system and as it systematically affects the end users.

The conceptual framework topics central focus among many of its subtopics that discussed the phenomenon of the safety message, that had been left prematurely vulnerable to attacks. Upon seeing most of the subparts and subtopics relate to safety messaging, as a key integrator to the problems about security and showcasing the intricate progressive problems that go beyond communication engineering, electrical computation, software, and cybersecurity. The exploration of the improvements of safety messaging system was a long-standing conceptual framework, which were a part of Vehicle Ad Hoc Networks (VANETs), and Automotive Informatics Security, sequentially that dove into a much deeper measures that distinguished apparent distinctions of general practices of subject matter experts and entailed to leverage their knowledge, skills, and abilities (KSA) of the phenomenon and harvested distinctive improvement frameworks.

Significance of the Study

The confidentiality, integrity, and availability of information transmitted to vehicular systems particularly the safety messaging system were shortly becoming the automotive manufacturer's problem. With an interest to ensure embedded systems, telematics devices, and automotive data were protected, automotive organizations must realize either how effective or how flawed their security posture were against its enemy's attacks and implementation of automotive systems itself. New technologies, such as assistive technologies, artificially intelligent systems, vehicular communications, and in-vehicle applications all sort to be exposed from the dangers of an impending attack—whether it be state-sponsored, service high-jacks, or malware intrusion to debilitate an operator's ability to navigate the vehicle singlehandedly. Should crises continue, a significant effort from the automotive industry, its partners, and data providers should provide mitigation efforts to advert risks that may endanger the registered motorist (Amin et al., 2015). The literature reviewed discussed themes of confidentiality, integrity, and availability and how the integral structure affected production and end-user at large, in within Chapter 2, and how prioritization efforts of improvement mechanisms were shortly needed for affected components such as the safety messaging system.

Conditionally, the automotive manufacturers had the upper hand in deciding whether they plan to accept being vulnerable, and or deem themselves protected when these kinds of flaws surface within the safety messaging system. While Amin & Tariq's analysis of the intrusive manufacturer-supplier approach helped reduced cybersecurity vulnerabilities and created significant strides to the privacy and protection of the motorist using well-architected secured vehicles, the demand for substantial impact were noted by the stakeholders and should increase improvement mechanisms through industry-based *security-by-design* argument in the coming vehicle implementations. The literature reviewed discussed themes of manufacture-based implementation and topics that organizations provide to increase technology and management symbiotic relationship, in within chapter 2.

Researcher Positionality and Reflexivity

The author of this research acted as the primary investigator with his current and established relationship within the automotive sector as a cyber vendor as captured studies explained the concurrent practices and problems within the safety messaging systems. In this role, the author's position was responsible for planning, developing, organizing, implementing, directing, and evaluating the selected method from qualitative research with the exploration of automotive vehicle security improvement framework (VSIF) on safety messaging systems through performance evaluations, particularly on the vehicle-to-vehicle systems and Vehicle Ad Hoc Networks (VANETs). The author was also actively participating in the development of Audi's big data lake infrastructure and programs as a strategic partner through his entity, but particularly from the perspective of the impact of information security within in-vehicular networks.

In this research, the author was responsible for translating the strategic and tactical business systems, engineering improvement plans, operational plans as it provide a purview to the improvement methods expressed, vehicle security improvement framework (VSIF) with the safety messaging system to protect against external hackers, as that would provide long-term effects for future outcomes, integration plans, and security interventions within the vehicular manufacturer (organization). The author was responsible for evaluating and advising on the impact of long-range planning of new programs/strategies and regulatory action as those items impact the attraction, motivation, development, and retention of the people resources of the automotive manufacturing security. The author was also be responsible for developing improvement planning models to identify competency, knowledge gaps and develop specific programs for filling those gaps within the safety messaging systems.

Delimitations and Limitations

Miles and Scott (2017) described the term *research delimitation* as the scope of the study with establish parameters. Moreover, study delimitation also prevents the author from generalizing and stating the findings (Miles & Scott, 2017). The delimitations within the study were set at the vehicle security improvement frameworks (VSIF) in the safety messaging systems to protect against external hackers, particularly improvements within the cyber and communication domain. The boundary was limited to security improvement or hardening of the BSM. As it was determined by the author, primary investigator, and subject matter expert as one of the primary concerns within the automotive industries that require further study and intervention. The improvements were discussed due to the safety gaps arising within the segment of systems architecture and implementation of in-vehicular technologies. There are no delimitations and or exclusion on end users' demographics while experiencing safety messaging.

Miles (2017) described the term *research limitation* as the constraints to the study based on the research methodology and design. It is also where the constraints act as a force that cannot be controlled within the study. Moreover, study limitation also acted as the constraint within the research method (Miles, 2017). The limitations within the study were set only for *interview* qualitative method constraints of participants, design control, and geographical restriction. Within the study, the author had modeled and ventured out within the qualitative design model as the author does not have any co-authorship support that couldhelp within the process and the model constraints that would not allow a longitudinal study to better understand the changes and effects of improvements through the years of iterative technological changes through product versioning. There was a limited amount of time to showcase improvements, as such semi-structured interviews and other explorative functions were then maximized to limited time andscale.

Definition of Terms

Many of the terms discussed throughout the chapters of the dissertation may use engineering verbiage through Vehicle-to-Network technologies that have amassed within our realities as motorists, consumers, and end-users. The technology, herewith, being described upon through the definition of terms predates years of extensive technological research and revolutionary frame working within Vehicular Ad Hoc Networks (VANETS). Described are the six vehicle connectivity types and pillars that have been revolutionized through the Internet of Vehicles (IoV):

Vehicle-to-Vehicle (V2V)

Zeadally et al. (2020) defines Vehicle-to-Vehicle (V2V) communications as being used in connected network to reduce traffic congestion, improve passengers' safety, and enable the efficient management of vehicles (Zeadally et al., 2020).

Vehicle-to-Infrastructure (V2I)

Xiong et al. (2020) defines Vehicle-to-Infrastructure (V2I) communications as the bidirectional exchange of information between vehicle and road infrastructure. V2I communication is used to obtain surface adhesion coefficient, road roughness, traffic lights, lane markers, road signs, and many accidents (Xiong et al., 2020).

Vehicle-to-Device (V2D)

Vehicle-to-Device (V2D) communication consists of a bidirectional exchange of information between a vehicle and any smart device. The technology provides the ability to wirelessly communicate and exchange information about navigation (Apple's CarPlay and Google's Android Auto), infotainment system, wearable data, and in-vehicular safety data.

Basic Safety Message (BSM)

Ahmed-Zaid (2019) defines Basic Safety Message communications as being used to interpret time, latitude, longitude, elevation, position accuracy, speed, heading, acceleration, yaw rate, steering wheel angle, transmission state, brake system status, vehicle size (length and width), path history and path prediction, event flags (hard braking, traction control) and exterior lights all was introduced as a standard through SAE J2735 (Ahmed-Zaid, 2019).

Dedicated Short Range Communication (DSRC)

The Federal Communications Commission (2022) defines Dedicated Short Range Communication as being used to communicate between vehicle-to-vehicle and vehicle-to-infrastructure communications helping to protect the safety of the travelling public as it can save lives by warning drivers of an impending dangerous condition or event in time to take collective evasive actions (FCC, 2022).

Vehicle Ad Hoc Networks (VANETS)

Brooks and Deng (2012) defines Vehicle Ad Hoc Networks communications as a type of mobile ad hoc network that comprises self-organizing vehicles as mobile nodes Vanet, which encompasses of vehicle-to-vehicle (V2V) and/or vehicle to-roadside (V2R) communications has been proposed for enhancing safety (i.e., collision avoidance, traffic optimization, lane changing assistance) and comfort (i.e., toll, parking payment, internet access, locating fuel stations) (Brooks & Deng, 2012).

Chapter Summary

Chapter 1 explained the definitions of terms required for the study: Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers, the conceptual framework design, along with the selection of a qualitative exploratory research. Conditionally, as passengers, motorists, and now end-users of vehicles, we were bound to and accustomed to the technologies we used to get within our destination. One of the technologies most predominantly used and important for passengers within the Vehicular Ad Hoc Network (VANETs) segment was the safety messaging system. This system, although conventional, within its exchange and delivery of traffic information, accident information, weather, speed limits, warnings, speed traps, and potential accidents etc. can be problematic and requires extensive security analysis, as well. With the study of the susceptibility of the safety messaging system towards hackers, research provided solutions and improvement models within the next generation of development, production, and post-production of automotive manufacturing and transit authority fleets.

In the following chapter, Chapter 2, the author of study, primary investigator, identified and reviewed the literature as it affects the study: Exploring Vehicle Security Improvement Frameworks in the Safety Messaging System to Protect Against External Hackers**.** Within Chapter 2, introduction to the review of the literature are identified, literature search strategies have been enumerated much throughout the section to identify many facets of many selected topics such as: (a) vehicle system architecture, (b) safety system architecture, (c) safety algorithm contributors, (d) safety messaging system issues, and (e) safety messaging aspects that must be resolved are brought about in depth to introduce vulnerabilities within in-vehicular systems, and particularly safety messaging. The gaps in literature and alternate scenarios have also been purposely discussed about in within the segment of the Chapter 2.

Moreover, much throughout the sections of chapter 2 showcased how in-vehicular networked systems were susceptible to the imminent threats of an external attacks, an event that could be elaborately planned by a sophisticated attacker, while exposing major auto manufacturing issues, through exploited backdoors gained by professional network of hackers, state sponsored attacker, and blackhat with their ability to specifically exploit challenges in engineering, owing to high mobility, and constantly changing topologies, can be very difficult for data communication to be accurate, exclusively in real-time as if propagation delay was expected from the system. Many technologies that affect the emergency messaging such as region of interest, the kinematic status of other vehicles within intermediate vicinities, potential or hazardous conditions within a mile stretch, congestion, all may affect the basic messaging system (BSM), safety messaging system, that will also require to prioritize an in-depth mathematical value engineered to a vehicular driver's end-users reaction time (Sou, 2012).

Distinctively, exposures can be an elaborate display of weakness. And as manufacturing organization have seen apparent demise from early integration of basic messaging system, an elaborate approach to vehicle security improvement framework (VSIF) must be achieved to curb future system malfunctions due to a backdoor attack from within the Internet of Vehicles (IoV). Controlling availability of and distinctive product feature set that may further showcase data transparency to the end user can be ultimately safeguard an already obscure and complex communication systems. The ability of manufacturers, and many subject matter experts, and state and federal government mandate, will be required to march against the security deficit against auto manufacturing of embedded system.

Chapter 2: Review of the Literature

The purpose of the proposed qualitative study was to explore vehicle security improvements framework (VSIF) in the safety messaging system to protect against external hackers. The research participant consisted of at least 6 subject matter experts as participant respondents who were qualified and expressed interest in the study as participant respondents. Participant respondents, particularly the human subjects, would fall into the category of Subject Matter Experts (SME) that were able to generally answer and pass certain knowledge, skills, and abilities (KSA) as they affected the formulation of safety messaging systems and make contribution to the domain. The subject matter experts who attended the research were the following: (a) network and security operators, (b) cloud system management providers (c) and transit authority executives who understood and verified effectively and effortlessly the problems and vehicle security improvements through their positioning within the automotive industry and public transit authority in term of safety and security of vehicular devices and critical product attachedwithin.

Literature Search Strategies

Materials within the Review of the Literature section were gathered and reviewed from an academic database, peer-reviewed journals, conferences, and seminars, and practitioner-grade manuals, within the Colorado Technical University - Doctoral Library, that may include but not limited to the attached reference list. Supplementally, standard reports, and information were gathered from practitioner-based reports, knowing that it would give light to the central phenomenon and would capture a great deal on the historical campaign to modernized approach on answering the question.

Vehicle System Architecture

Seigel, Erb, and Sarma (2018) expressed that the art of connected vehicles is heavily reliant on complex electronic networks (Seigel, Erb, & Sarma, 2018). The authors have pointed out the inter-vehicular networks such that resembles of mesh networks (Mallikarjuna Rao, Subramanyam, and Satya Prasad, 2018) is one of the primary concerns when it comes to VANET testing and deployments (Mallikarjuna Rao, Subramanyam, & Satya Prasad, 2018). Certain network capability must be looked upon whenever they deploy such as: (a) communication standards, and lastly (b) broadcast types as these technologies connect devices to in-vehicular systems. Conditionally, the broadcast types assist in managing interoperability of communications and is distributed in safety messaging system unit that allows different types of emergency communication to affect position-based transmission that can emit: (a) beacon messaging (Enis, 2015), (b), flooded messaging, and (c), GeoCast messaging (Hall, 2013) which play a pivotal role in broadcasting and relaying emergency messages (Enis, 2015; Hall, 2013; Seigel, Erb & Sarma, 2018).

While it can be argued that networks can be the top priority in building a web of standards for vehicular and direction-aware architecture (Haider, 2020). The system design can also be an integral source for safety systems and human-machine interaction models (Madrigal & Frederic, 2020). Additionally, it is a much rather complex and increasingly sub-functional system due to the confluence of on an already involved electro-mechanical network (Wu, Li, and Qin, 2021). This vehicle systems include the following: engine, framework, electrical power, power plant, and hydraulic, and safety system that must be conveniently tied up together to purposely function within the vehicle system architecture (Haider, 2020; Madrigal & Frederic, 2020; Wu, Li, & Qin, 2021).

Vehicle systems interdependently and mechanically sourced together play a part in the build of a strong vehicle network, though the parts of the vehicle such as engine system (Lu et al., 2011) framework system, electrical power system, powerplant system, hydraulic system, and or safety system must play a key role in delivering a system broadcast messages within the vehicle aware networks (Lu et al., 2011). Tas et al. (2017) suggested that in a DARPA Urban Challenge, the performance monitoring system implemented in the winner vehicle, Boss, monitored the progress in its mission. If the mission was repeatedly obstructed, it issued recoveries (Tas et al., 2017).

Boukerche and Zhang (2019) explained that the vehicular nodes are capable of transporting, sensing, processing information, and wireless communication, which makes them more vulnerable to worm infection (Yao et al., 2018; Bourkerche et al, 2019) and conventional hosts. The researchers have stated that in itself wireless communications are susceptible, in particular the vehicular systems, or that they can be hijacked by an adversarial attacker (Boukerche & Zhang, 2019; Yao et al., 2018; Zhang & Li, 2020). Increasingly, the worm infections were resealed within the VANETs, and results regarding accessing safety systems have been profoundly significant which then affects total vehicle operations (Khan & Chowdhury, 2021) by the driver and the end-suer total experience within the vehicular unitand the vehicular platform (Khan & Chowdhury, 2021). The aforementioned research went through V2X communication (WU, Liu, Yang, Shan, and Quek, 2021) application and propagated worms to show the indispensability of the characteristics of worms against VANETs (Boukerche & Zhang, 2019; Wu, Liu, Yang, Shan, & Quek, 2021).

Secondly, the researchers were able to explore certain attack vectors perpetuated by worms which had spread over Vehicle Ad Hoc Networks (VANETS). The researcher had determined significant increase of such vulnerable backdoors through correlation with time as more in-vehicular systems are shortly becoming less electrical and more software-based products. Lisok (2016) expressed that the U.S. National Highway Traffic Safety Administration (NHTSA) wants to take steps to secure communication within vehicle-to-vehicle (V2V), in able for vehicles to talk to each other effectively (Lisok, 2016). Meanwhile, the worm infection has made the VANETs a reputable host for infection, controlling certain aspects of the daily operation of the driver and end-user, and increasingly slowing the pace for end-to-end communication, and deliberately hampering vulnerability management.

Limbasiya and Das (2019) discovered that the vehicular system, in particular the safety system, must meet a certain standard of a certificate-based system, for vehicles to regularly change/update their private/public key to provide secure data exchange between two entities. Therefore, the system should have a massive storage capacity and sufficient power to provide services at times (Limbasiya & Das, 2019). The researchers uncovered that for vehicular in-networking to function, especially hosting user-initiated and server-initiated PII, sensitive information must be masked from a safety system, and should only be opened by the intended participant in most cases anonymizing data (Yu, Ni, Yu, Zhang, and Liu, 2021) to a current user from reaching other's PII, except if they have the proper authorization, and private/public key to open/ secure data (Yu, Ni, Yu, Zhang, & Liu, 2021).

Oh et al. (2021) suggested that as technology advanced, with such asinfotainment systems being one of the most proponent functionalities implemented in a vehicletoday, driver's attention is diverted to control these systems, causing fatal accidents, making human interaction more significant and important with safety workflow of safety messaging, inherently connected with infotainment systems. Many of the functionalities such as voice, continuous-wave radar sensors, thus require low complexity for application to vehicle environments as resource-constrained platforms (Oh et al., 2021). These technologies are programmed to adapt with human interaction in demand, required for drivers to use safety systems, during movement increasing such human interaction with thesystem.

Safety System Architecture

Costigan and Lindstrom (2016) discussed the increasing level of importance of the national security agenda, as it illuminates modern-day technologies from a vehicular safety system, to include physical and virtual worlds of cybersecurity (Costigan & Lindstrom, 2016). The agenda repeatedly calls for the merger of sensors and computing devices, that total in billions, to connect objects in a network that does not require human intervention. The researchers also discuss increasing security threats on devices that will create unsurmountable vulnerabilities in the digital world. Secondly, the Internet of Vehicles (Ghafoor, Kong, Zeadally, Sadiq, Epiphaniou, Hammoudeeh, Bashir, and Mumtax, 2020) primarily the one that relates to vehicle-to-vehicle (V2V) communication, succinctly related to safety and security of devices, have to be protected (Ghafoor et al., 2020). The authors have noted the present opportunities for revolutionizing the in-vehicle internet or Internet of Vehicles (IoV) for motorists end users and vulnerable road users. The authors introduce policy and trends for vehicular IoT and its significant trend within the next decades to come. Strengths towards security implications in the IoT revolution have been an important keystone for the agenda, however, weaknesses in mitigating risks and challenges were not overcome in the indicated policies (Costigan & Lindstrom, 2016).

Milosevic et al. (2019) proposed that one of the goals when increasing autonomy of the vehicle is to increase the safety of drivers and other participants in the traffic (Milosevic et al., 2019). The authors note that 95% of all accidents are initiated by driver error. Moreover, manufacture-based implementations suggest the use of Advanced Driving Assistance Systems (ADAS) (Yin et al., 2018) applications connected to all safety operations of the vehicle (Yin et al., 2018). With that regard, ADAS has been configured to include sensors, algorithm, network, and storage capability to increase reliability toward vehicle networks, much so enable safety tracking for in-vehicular built systems (Milosevic, Isic, Bjelica, & Andjelic, 2019). Though, much of the granular aspects of the safety system, with a resonance of open networks can prematurely open a backdoor (Thimmaraju, 2021) for mere adversaries (Mousavinejad, Yang, Han, Ge, and Vlacic, 2020), blackhat, greyhat operators, and other nation-state or sponsored-attackers (Thimmaraju, 2021; Mousavinejad, Yang, Han, Ge, & Vlacic, 2020). Meanwhile, the connectedness of the context-aware vehicular networks (Liu, He, Wensowitch, Rajan Dinas, and

Camp, 2020) not only considered to be intelligently been productive for manufacturers but also problematic against information and data leakage (Liu, He, Wensowitch, Rajan Dinas, & Camp, 2020). More so, the critical units of operation can also be succinctly tracked by data providers without proper privacy authorization and management, data snooping could propagate widely and in turn be referenced by many blackhat and greyhat operators.

Nouh et al. (2021) suggested that the Internet of Vehicles and the most recent technologies adapted to intelligent vehicles must ensure road safety by preventing and detecting road accidents more accurately (Nouh et al., 2021). The researchers recommended that the dynamic personalized analysis of driving behavior is possible when traffic data is available and processed together with advanced AI technologies. Meanwhile, in a study by WHO, almost 1.35 million people die each year as a consequence of road accidents and a large quantity of the population suffers from road accident injuries, which therefor affect human losses (Nouh et al., 2021). Consequently, road traffic accidents are due to human error and are most likely preventable if safety messaging system is a standard feature of a safety system, therefore available within reach of the vehicular setting, and not considered as an option for most auto manufacturers. Much of the demise, of the large quantity of the population, is the inability of automotive companies to communicate safety features at a rigorous level to consumers who are looking to purchase a new unit of a vehicle.

Knowles-Flanagan et al. (2021) described SAE International's definition of one of the VANET's key sub-features as Basic Safety Message (BSM), which can be vital to the safety-related information passed to drivers, such as location, speed, heading, and general operation details (Knowles-Flanagan et al., 2021). The type of messaging transported to these nodes is defined as a broadcast message. The BSM is also called, or also known as a Cooperative Awareness Message (CAM) in some regions, and countries, but acts as the same as the safety messaging system for most vehicles (Knowles-Flanagan et al., 2021) Indeed, the Safety system is included within the complex workings of the safety messaging system, and to whatever the nomenclature, designed platform, or theoretical concept, the information must be passed to the vehicular network and be viewed by the driver (end-user). Much of the problem begins when such BSM does not communicate with the intended audience, due to perpetrator interception, electrical node error, and miscommunication within networks that the driver was not fully aware of.

Aneetha and Sundan (2015) expressed that the expanding safety system communication requirements in today’s world demand extensive and efficient network systems (Aneetha & Sundan, 2015). The researchers provide effective security protocols for the network environment, as its primary methodology in security attack vectors (Haber, Morey, Rolls, and Daran, 2020) and possible vulnerabilities. The implementation of intrusion detection systems to capture the network traffic and log information to include Multivariate Hotelling’s Statistics made attack detection live to conduct traffic profile, and testing (Haber, Morey, Rolls, & Daran, 2020). The research provides effective detection rates (Lu, Han, Ren Dai, and Li, 2018) and false alarm rates better than previous approaches (Lu, Han, Ren Dai, & Li, 2018). Strengths showcased in the research were thee cross-validation of various models, while its weakness did not show characterization of industry-approved intrusion detection, as it was still in the experimentatal phase (Aneetha & Sundan, 2015). Meanwhile, Sugumar et al. (2018) shared that there is a proficient solution for network safety that was developed by using electronic signature and applying encryption mechanism on every location service packets, by not interfering in the fundamental process of location service (Sugumar, Rengarajan, & Jayakumar, 2018).

Durech et al. (2016) modeled security principles that reflect on system architecture, and the sphere of vehicular networks that concentrated mainly on the following areas: routing protocols, power of antennas, elimination of error rate, control of mobility, the realization of database systems but also on the solution of security architecture on the base of modern cryptographic constructions using PKI (Public Key Infrastructure) and Cas (Certification Authorities) (Durech, Franekova, Holecko, & Bubenickova, 2016). The researchers expressed the study of modern cryptographic frameworks is insurmountably becoming a model for more and modern-day vehicular architecture. But, without so much exposure to a considerable amount of threats involved within today's vehicular internet mobility (Tu, Wang, Zhang, and He, 2021) environment, implementation would be a cause of concern to many auto manufacturers that have not evolved their in-vehicular security, particularly that technology that affects mostly data communications, like the safety messaging, or predominantly known as basic safety message (BSM) system (Tu, Want, Zhang, Zhang, & He,2021).

Loupis (2014) determined that embedded systems technology has perhaps been the most dominating technology in high-tech industries, in the past decade and today. The researcher explores the versatility of application in the embedded system arena. The author notes that most adopted software methods yield high-quality design and process structure. The research presents a MODUS-oriented market analysis n the domains of Formal Verification tools, HW./SW co-simulation tools, Software Performance Optimization tools, and Code Generation tools. The research expands on the current market overview and its size across all regions, determining the importance of current embedded system technologies. Certain strengths were apparent in the qualitative research, such as the introduction of MODUS oriented analysis and other tools. The weaknesses involve performance optimization and quality strategies that were less significant for the embedded software system (Loupis, 2014).

Safety Algorithm Contributors

Kang and Kang (2016) introduced novel research about intrusion detection systems (IDS) using a deep neural network (DNN) (Srihari, 2021) to enhance the security of an in-vehicular network (Kang & Kang, 2016; Srihari, 2021). The authors provide a probability-based feature vector that can extract network packets from the in-vehicular system. In return, the DNN can provide a probability of each class discriminating normal and attack packets (Deng, Gao, Lu, and Gao, 2018), thus, the sensor can identify malicious attacks on the vehicle (Deng, Gao, Lu, & Gao, 2018; Eziama, Awin, Ahmed, Santos-Jaimes, Pelumi, & Corral-De-Witt, 2020). The research conducted an unsupervised pre-training method of deep belief networks (Wang, Qiao, Liu, and Shen, 2021), to include the stochastic gradient descent method (Sun, Qiao, Liao, and Li, 2020) can extract in-vehicular network packets (Wang, Qiao, Liu, and Shen, 2021; Sun, Quio, Liao, & Li, 2020). The research outlines related work for CAN protocol, which includes intrusion detection and machine learning, deep learning, a proposed technique for a proposed intrusion detection system, CAN packet feature, attack detection, data set, and performance evaluation. There are no significant weaknesses proposed in the article (Kang & Kang, 2016).

Zaidi et al. (2016) proposed and evaluated an intrusion detection system (IDS) for vehicular ad hoc networks (VANETs). The IDS is evaluated by simulation in the presence of rogue nodes (RNs) that can launch different points of attack. Meanwhile, the proposed Intrusion Detection System is capable of detecting a false information attack using statistical techniques effectively and can also detect other types of attacks (Zaidi et al., 2016). Moreover, the researchers have reached a consensus that the theory and implementation of the VANET model used to train the IDS has been productive yet cumbersome through much of the implementation processes. Secondly, the RNs are introduced within the network and presented as an algorithm to detect the false likelihood of an attack. The researchers have evaluated that proposed architecture must be introduced within the application layer for information exchange and dynamic fast-flowing networks, in the purpose of VANET (Zaidi, Milojevic, Rakocevic, Nallanathan, & Rajarajan, 2016).

Bouali et al. (2016) stated that vehicular environments remain vulnerable to various potential attacks because of continuous interactions and information exchange between vehicles despite the deployment of authentication techniques by communication standards. Therefore, an authenticated node with a certificate could initiate an attack while complying with implemented protocols (Bouali et al., 2016). The researchers had expressed that some mechanisms enhance communication technologies, including a preventive mechanism such as Intrusion Prevention System (IPS) can filter and predict vehicles behavior. The researchers have proposed that the Kalman Filter algorithm can be used to predict the future health of vehicles' behavior as it can also classify them into three categories: (black, grey, and white) based on trustworthiness (Bouali, Senouci, & Sedjalmaci, 2016; Peksa, 2020).

Kolte and Madnkar (2014) articulated that vehicular ad hoc network (VANET) is one of the recent and promising technologies for revolutionizing the transportation system where vehicles can communicate by sending a message with each other via a wireless medium (Kolte & Madnkar, 2014). The authors have noted that the primary motivation of vehicular communication is not only to reduce the number of traffic accidents but also to decrease traveling time, congestion, etc. by setting implementation on various traffic-aware applications (Kolte & Madnkar, 2014). Interestingly, vehicular communication can certainly be affected by incoming adversaries, nation-state attackers, and external hackers trying to pin on communication and siphon critical information to centrally control vehicular networks.

Moreover, vehicle manufacture-based implementations are increasingly being remodeled as open networks for vehicle-to-vehicle frameworks to function, to the very least.

Park and Kim (2013) elaborated that for safety messaging in a vehicular networking environment, strict messaging frequency requirements must exist. For this issue, the researchershavetoutedatleast6outofthe8cooperativevehicularsafetyapplications,chosen by the National Highway Traffic Safety Administration and the Crash Avoidance Metrics Partnerships, require a minimum of 10Hz, whereas the pre-crash sensing application requires an even higher frequency of 50 Hz for messages that convey the positions of vehicles. Currently, the researchers have finalized the collisions of periodic safety message broadcasts for theIEEE

Wireless Access in Vehicular Environment (WAVE) system that must be left to the IEEE 802.11p medium access control (MAC) to resolve. With a small convention window, it is stipulated at 802.11p, however, MAC only offers limited relief to the collision problem (Park & Kim, 2013).

Zhang et al. (2020) expressed that there have been significant changes within the collision warning algorithm. The existing collision warning algorithms are mainly divided into two categories, namely the safety time algorithm and the safety distance algorithm. The safety time logic algorithm compares the collision time between the two workshops with the safety time threshold to determine the safety status. The safety time algorithm mainly uses Time to Collision (TTC) (Urban & Caplier, 2021) as the research object. The safety distance model refers to the minimum distance between the vehicle and the obstacle, which is also the distance the vehicle needs to maintain to avoid the collision (Zhang, Du, Wang, & Wang, 2020; Urban & Caplier, 2021). Subsequently, the use of the safety distance algorithm significantly reduces time to impact, while ensuring the safety of the end-user and driver, as well.

Liu and Yu (2009) examined the related algorithm of an integrated navigation system on a presented vehicle. The algorithm analysis exposed navigate solutions such that of altitude, position, and velocity of the vehicle. The authors have found out that intelligent vehicles rely heavily on remote sensing, information fusion, system integration, estimation, and identification to manufacture intelligent vehicle navigation platforms (Liu & Yu, 2009). Though the series of technologies only open a web of information-aware and vehicle-aware networks to be much overpromised with safety, information leakage is far more prominent within the classification of open networks.

Kang et al. (2020) approached that the primary advantages of the global navigation satellite system (GNSS) with the use of the global positional system (GPS) and the use of LiDAR sensor will require that light be detected within the range of curbs, road shapes, rails, vehicles, and road infrastructure. Employing LiDAR allows for laser signals to be directly measuredwithin the distance. The sensor can provide a 3-dimensional representation of the environment and that the installation of sensors will provide advantages to end-users and drivers, while systematically uploading a 360-degree view of the driving environment (Kang, Min, Yoon, Kim, & Park, 2020). Meanwhile, the 3D rendering of the view can also be uploaded through the cloud, to collect data that would ultimately keep safety a priority for drivers, both physically and digitally. However, an unventured area where vehicle-to-cloud (Sliwa, Falkenberg,Liebig, Piatkowski, and Wietfeld, 2020) data can be manipulated in such a way that affects the end user's response while driving, could ultimately lead to accidental claims, from operational sabotage to accidental deaths due to an increasing manipulation, machine-learned data that have been provided by an adversarial attacker, or an error on data manipulation (Kiss, 2019), or through consistent machine malfunction (Sliwa, Falkenberg, Liebig, Piatkowski, & Wietfeld, 2020; Kiss, 2019). Moreover, the distinguishing fact that the 3D data are consistently being uploaded to the cloud could lead to an overwhelming amount of problems with privacy in such a way that would lead the end user's data unchecked and user's location available elsewhere for an unhinged attacker to manipulate vehicular operation.

McDonnell et al. (2021) addressed that vehicles fitted with telematics devices often can introduce efficiency benefits, either through optimized driving techniques, or improved traffic flow. Telematics is capable of data broadcasting information through the GPS, announcing speed and emergency alerts through traffic-aware areas, and or smart intersections. Most of these devices are connected to what is called Signal Phase and Timing (SpaT) systems which can broadcast speed and GPS data for data-enabled vehicles, enabling vehicle optimization in real-time events. Energy efficiency can be achieved by the usage of network systems and optimal driver behavior is provided with feedback systems to improve the overall fuel efficiency of a vehicle, as well (McDonnell et al., 2021).

Safety Messaging System Issues

Petit and Mammeri (2013) researched increasing passenger safety by exchanging warning messages between vehicles wirelessly. The research involves resisting various malicious attacks and analysis on authentication algorithm (ECDSA) was performed to see the impact on vehicular network performance. The algorithm concluded authentication time overhead. The algorithm was calculated for modular and scalar multiplication (Guo and Bei, 2021), modular inversion, time complexity, and communication delay (Petit & Mammeri, 2013; Guo & Bei, 2021). Certain strengths in research simulation provide a potential vehicular safety mechanism to improve the driving experience, while weakness includes the security mechanisms itself, which has overhead that affects the performance of vehicle-to-vehicle (V2V) functions (Petit & Mammeri, 2013).

Gyawali et al. (2020) suggested that vehicular networks are vulnerable to various attacks such as Sybil (Bochem and Leiding, 2021), denial-of-service (DoS) (Xiao, Ge, Han, and Zhang, 2021), and false alert generation attacks. Cryptographic methods can provide some protection to vehicular networks from external attacks but are found to be vulnerable to internal attacks (Gyawali et al., 2020; Xiao, Ge, Han, & Zhang, 2021). A misbehavior detection system (MDS) can be deployed to detect and prevent internal attacks (Gyawali, Qian, & Hu, 2020). The researchers have employed that most in-vehicular network providers, particularly are more concerned about the safety of vehicle-to-vehicle safety messaging, and with the allowance of manufacture-based processes, may ultimately either contribute to safety and welfare of the end-user and drivers within the seat. However, deploying on-demand security (Chung, Kim, and Jeon, 2016) professionals to take on misbehavior detection systems will require certain knowledge and functioning of the algorithm and framework (Gyawali et al., 2020; Chung, Kim, & Jeon, 2016).

Koops and Leenes (2014) expressed the importance of privacy by design, which promotes the concept of safety messaging system privacy on newly built in-vehicular systems. The authors present an increasing need for general data protection regulation to equip businesses and software products before deployment. The authors argue the importance of embedding data protection (Daneshmandpour, Danyali, and Helfroush, 2019) requirements in system software necessary for extreme interpretation and hardening of critical assets (Daneshmandpour, Danyali, & Helfroush, 2019). The weaknesses and previous problems from past developments engaged the author to induce privacy by design, to answer for extensive threat exposure and vulnerability of information subjected towards the end-user (Koops & Leenes, 2014).

Amin and Tariq (2015) examined the current security posture of newly released in-car systems produced by automobile manufacturers, rendering vulnerable hotspots for cyber attackers. Vulnerable systems were documented from sound systems, Bluetooth modules, onboard diagnostics systems, cellular communications, and the bus connecting electronic units, according to its researcher. Invaluably, the author notes that the challenges from new in-car systems come from the delivery of its ecosystem, outsourcing manufacturers to provide top features for end-user —the motorist. The article also provides a certain solution to the designated weaknesses, which states: (a) encryption of communications, (b) anomaly detections, and (c) improve the integrity of embedded software (Amin & Tariq, 2015). Their discovery also provides certain solutions against designated weaknesses, which states: (a) encryption of communications, (b) anomaly detections, and (c) improve the integrity of embedded software (Amin et al., 2015).

Wright (2011) conducted research that involve the hacking of vehicular technologies. The author exposed certain threats, vulnerabilities, and exposures to in-car systems designs that were manufactured by embedded system partners. The author notes the importance of secure communication techniques that would increase the integrity and security of stored information. The author showcases undisclosed hacks of vehicles to involve monitoring of police car video feed in real-time. The author associates the real-time effects of the undisclosed hacks with automobile manufacturers' new technologies. The author calls for expansion of security hardening to embedded software applications within the in-vehicular carsystem.

Certain weaknesses were assessed and were verified by cybersecurity research consultants and calls the need for additional research to cover embedded telecommunications, in-car system software design, and manufacturer involvement in security by design integration (Wright, 2011).

Amel and Guizani (2019) distinguished only the attacks targeting the routing protocols. In these attacks, a malicious node exploits the vulnerabilities of the network layer by dropping packets or disordering the routing process of the network to disturb the network. To prevent such attacks and to protect the network, the desired requirements in VANET are vehicle authentication, vehicle privacy and anonymity, message integrity, message non-repudiation, message confidentiality, and service availability (Amel & Guizani, 2019).

Safety Messaging System Aspects that Must be Resolved

Jackson (2020) explained that one of the key challenges within a safety messaging system standpoint is ensuring that the data is being delivered to its intended location, that delivery of information, be it to the vehicle, or from the vehicle out to the network, happens without delay. Krishna Jayaramen, head of connected vehicles, mobility for Frost & Sullivan explained the current data demands for connected vehicles is not a major issue, however, the evolution of autonomous vehicle capabilities will present a major challenge for the future of vehicular technologies (Jackson, 2020). While the networks expand as the demand for the newer in-vehicular system as part of a new market entrant of most major automotive manufacturing grows, associated technologies that elaborately make development much easier for systems architects easier, pose a significant threat as the reliance on interconnected systems keep most systems downgraded to open networks, making it much easier to penetrate an adversarial attack within the safety messaging units.

Casal (2005) concluded that in-car communications systems can contribute to the confluence of surveillance-rich environment, where it is the pervading norm of today's privacy posture. The authors note the pervasive approach to include electronic health records in emergencies, and user's location processed inside the telematics device transferred in an event of emergency. The research highlights in-vehicular systems' current privacy conflicts that may arise in very specific circumstances. The author calls for privacy laws within passenger data and in-vehicular car systems. The research analyzes the car manufacturer's guidelines for privacy protection and European Union's privacy directives. The author concludes that the in-car systems are eroding privacy in a big way. Strengths in observations methods such as data subjects were not able to control the personal information collected about them, and too many data sources were unchecked and uncleaned which made a huge security impact, much so affecting the privacy of the driver. The lack of regulation subject drivers and users to accept a loss in privacy. Weakness in strategy and privacy modeling was significant and could be better improved for future research (Casal, 2005).

Hathal et al. (2020) explored that using VCS, vehicles can form a dynamic self-configuring network that enables a vehicle to communicate with other vehicles (V2V) and roadside infrastructure (V2I). However, such wireless communication channels are vulnerable to attacks, and therefore an authentication scheme for communications should be designed before the deployment (Hathal, Cruickshank, & Maple, 2020). Safety messaging systems areleft undesired with a tumultuous amount of threats therein the in-vehicular wireless networks. Considering the security framework and protocols to implement, leaves system architects identifying appropriateness of authentication schemes for the end-user, driver, and primary stakeholders of any automotive manufacturer (Hathal, Cruickshank, & Maple, 2020).

Ioana and Korodi (2020) expressed that premium cars have more than 80 ECUs and the demand for inter-ECU communication has increased greatly, in great effect toward vehicular technology revolution. In the current vehicle architecture, the gateway is the only device that ensures network communication between different networks. The gateway is one of the most important components for distributed applications and must assure that messages transmitted over the network meet their constraints (Ioana & Korodi, 2020). The researchers found that an increasing layer of communication network support, protocols, and framework must substantially be increased to protect against network sniffing from perpetrators, adversaries, nation-state, and or blackhat attackers looking to enforce backdoor penetration against vulnerable systems and assume guidance of toward the end-user and driver.

Yu et al. (2021) showcased that with the prosperity of vehicular networks and intelligent transport systems, the vast amount of data can be easily collected by vehicular devices from their users and widely spread in the vehicular to solve large-scale machine learning problems. Hence how to preserve the data privacy of users during the learning process has become a public concern. To address this concern, under the celebrated framework of differential privacy (DP) researchers have determined decentralized parallel stochastic gradient descent (D-PSGD) algorithms are used to process large amounts of vehicular data (Yu, Zou, Chen, Tao, Tian &

Cheng, 2021). The researchers have studied privacy with an increase in stochastic algorithms, to influence machine-based problems progressively indicated in more data-centered and safety-specific systems for in-vehicular networks. The researchers have also expressed that a safety messaging system where data can be prematurely be manipulated, must by all means be safeguarded against privacy concerns (Yu, Zou, Chen, Tao, Tian & Cheng, 2021).

Khayati and Mazri (2020) detailed that routing in the vehicular ad hoc (VANETs)network is a very difficult task due to its high level of mobility and the frequent disturbance topology (Qin, Bian, Hu, Sun, and Hu, 2020) of the links (Khayati & Mazi, 2020; Qin, Bian, Hu, Sun & Hu, 2020). Vehicular communications are very insecure in the face of various threats; security is, therefore, an important aspect of VANET deployment to make Intelligent Transport System (ITS) (Lv, 2020) services available to every end-user (Khayati & Mazri, 2020; Lv,2020).

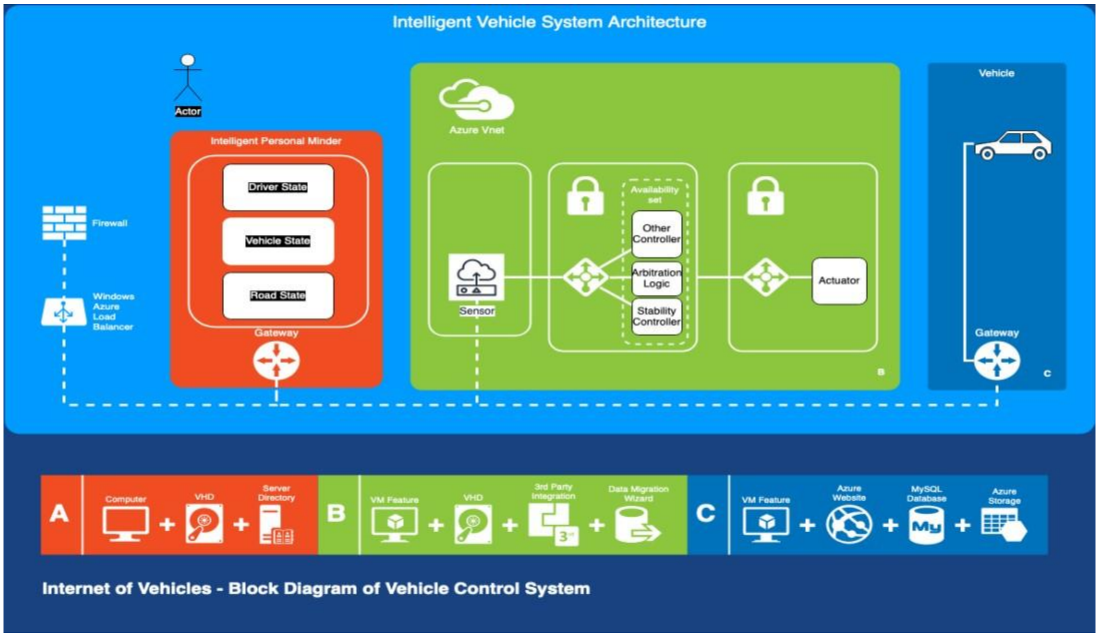
Meanwhile, the significant efforts by the researchers to ultimately understand the connectedness culture between V2X open vehicular networks have indicated that security within routing networks, in particular, the safety messaging aspect of the communication system has not been fully formalized nor has it been a framework to a key standard for in-vehicular networking. Moreover, this meant that the vehicular ad hoc networks are nevertheless filled with unsuspected threats, real-time vulnerabilities, and exposures that have not been patched simultaneously by the automotive manufacturers, in real-time. Succinctly, this creates unprecedented threat chains as the attack vectors become much known within the in-vehicular units.

Ibrahem et al (2021) suggest that to transmit and allocate safety information, the vehicle must be programmed to 75MHz in the 5.2GHz band for licensed dedicated short-range communication (DSRC) that should deliver high media contents to V2V communications, and should avoid V2V communication avoid costly RSU installation and take advantage of the VANET delivery of traffic information, and vehicular driver can receive a warning message from another vehicle when there is any hazard situation or risk of an accident (Ibrahem et al., 2021). However, if the dedicated channel range, and distributive allocation standard band of DRSC is tapped to give out and provide a different real-time transport of emergency communication, specific to address any current safety message would not be transmitted, in return the vehicle would not see the current accident coming in real-time, and the driver (end-user) would be placed in danger. Insecurity happens when the programmed allocations from DSRC do not match the standard for safety, while vehicle information is passed in a different allocation, it can be lost in translation and may never be able to reach the intended customer, driver, and end-user for all the effort sent through and built from the airwaves.

Sou (2012) expressed that due to the manner of how VANETs behave, specifically dueto challenging tasks, owing to high mobility, and constantly changing topologies, it can be very difficult for data communication to be accurate, exclusively in real-time if propagation delay is expected from the system. Many technologies that affect the emergency messaging such as region of interest, the kinematic status of other vehicles within intermediate vicinities, potential or hazardous conditions within a mile stretch, congestion, all may affect the basic messaging system (BSM), safety messaging system, that will also require to prioritize anindepth mathematical value engineered to a vehicular driver’s end-users reaction time (Sou, 2012). Due to the high mobility, propagation delay can result in inaccuracy and can further be a larger contextual problem, for the drivers using the safety messaging system of a particular automotive manufacturer.

Figure 2

Block Diagram of Vehicle Control System



Note. Intelligent Personal Minder including but not limited to Driver State, Vehicle State, and Road State, by Lu, Filev, Prakah-Asante, Tseng, & Kolmanovsky, 2009.

Lu et al. (2009) suggested that to understand real-time vehicle handling limit warning and driver style characterization, organization should understand the novel approach to driver advisory system that warns drivers of driving conditions close to limit of vehicle handling. Whereby, safety messaging system relies, the block diagram from above in Figure 2, p. 37, should show the Intelligent Personal Minder where Driver State, Vehicle State, and Road State are all attached in an overarching architecture between Intelligent Personal Minder and Controller System. For any control system, the plant model plays an essential role in designing an effective control. Similarly, a driver model is important for generating effective and appropriate driver advisory signals. Mutually, the driving style characterization is required to truly understand how vehicle logic and vehicle response adopt to end user's control. The safety messaging system adopts with the vehicle state and the road state and provides appropriate reminders and suggestions (Lu, Filev, Prakah-Asante, Tseng, & Kolmanovsky, 2009).

Gaps in the Literature

Xu et al. (2004) expressed that for much of the decade, automotive systems particularly the safety messaging system have become synonymous with vehicle-to-vehicle functions, with goals to send safety messages to other vehicles with high reliability and low delay (Xu, Mak, Sengupta & Ko, 2004). Meanwhile, while there have been so much attention placed building and integrating an adequate safety messaging system for end-users, there have been many in particular, challenges that makes the safety messaging threat-worthy to most resilient adversaries, backdoor attackers, and most nation-states, that may want to cripple critical infrastructure (Njotini, 2013) such as personal transportation (Njotini, 2013). Moreover, the focus of much debate and discussion within the industry has been to enhance feature-based technologies for the critical and safety messaging, merely not to expose significant threats that allow attackers to seek root access, but to elaborate on the long withstanding efforts of the systems architect to improve safety messaging system from end-to-end.

Consequently, there have been gaps that relate to the literature that have not been seriously given attention by the author, by most embedded system manufacturers, automotive manufacturers, and cloud-computing partners that hampers progress in achieving the ultimate goal of *security-by-design* (Chattopadhyay, Lam and Tavva, 2020) for automotive safety messaging systems (Chattopadhyay, Lam & Tavva, 2020). One of these gaps, in a relatively high likelihood, is the prioritization of the vehicle ad hoc networks (VANETs) safety messaging system through security system design (Yu and Luo, 2020) review (Yu and Lao, 2020).

Additionally, there had been much thought to design review a security architecture, after all, current literature, recommendations, and practical efforts have made safety messaging a primary target and host for attacks on vehicle systems. Conditionally, we have been too reliable as drivers and end-users, to automotive manufactures that implementations with safety messaging systems becoming an integral part of auto technologies. Much so, we less demanded and appreciated the significant control and hazardous effects of safety messaging system, had it not been effective or reliable introducing backdoors, in within the limits of a session hijacker, or adversaries that may control end user’s interface, while believing that everything implemented on most vehicles, at best are safe, not knowing the true nature and security posture of the safety messaging system while being very dependent on safety messaging systems, as it is equipped with much technology to predict outcoming crashes, end-point accidents, and EMS notifications. Altogether, this poses a bigger progressive problem, and how not a system design review could effortlessly change the implementation of a safety messaging system.

Conclusions

The review of the literature exposed that there are areas within Vehicle Ad Hoc Networks (VANETs) that indicated susceptibility to errors of communication due to engineering implementation, such that notifications have propagation delays, that can result in inaccuracy, secondary to high mobility and changing typologies. One of the most integral parts of the literature is the dissection of the vehicle system architecture, which had also described that basic safety message (BSM) system, or safety messaging system, has become an independent feature that could become a host target, too many adversaries, and many enemies foreign and domestic. While the purpose of the study was to reduce the susceptibility and to make recommendations for Systems Architects, exposing the risks has become a mere byproduct and fundamental framework for vulnerability management professionals. In doing so, we find that there are pathways for systems architects immediately control risk within the vehicle-to-vehicle communication.

Bhoi and Khilar (2012) expressed that insecurity is a core issue in Vehicle ad Hoc Network (Internet of Vehicles), and may affect particularly the segment of safety messaging system, because it is strongly becoming affected by most attacks (Bhoi & Khilar, 2012). Lately, this trend affects network performance as it leads to insecurity in data communication (Bhoi & Khilar, 2012). As automotive manufacturers, embedded systems, third-party data providers, architectural security engineering, and data custodial partners march to safeguard the overall confidentiality, integrity, and availability of information in our vehicle, it is important to acknowledge and examine the state of security these stakeholders partake in the fight for a more secure, safe, and protected product launches, to alleviate and recompense for security risks that may harm passengers (Amin et al., 2015).

While there are many more in store for VANETs, systems architects must loop into the most undesirable situation to inoculate the risk of harming motorist and end users during safety and emergent situations. While the purpose of the safety messaging system is simply to decode and calculate incoming vehicular messages that have been passed through the intraand extra- vehicular network, through vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-cloud communication, the consequence of getting a delay, forecasting an error, and cross-matching a mistake message could fall into the hands of an innocent lives, disarming motorist of their vehicular control and security, and could consequentially amass catastrophicdisaster.

Chapter Summary

Chapter 2 explained the literature review, vehicle system architecture, safety system architecture, safety algorithm contributors, and safety messaging system issues. The literature review also glossed around the breadth of knowledge and scope requirements required to operate safety messaging system, along with the exposure of operational and security weaknesses and threats that could be generally taken advantage by a trained professional hacker, penetration tester, or conventional systems architect that understands the mechanism of attack on the safety messaging device.

Sou (2013) explored that with a Vehicular Ad Hoc Network (VANETs), vehicles are able to communicate with one another through a technology called Dedicated Short-Range Communication (DSRC) wireless device. With cars build with at least hundreds of smartsensors, vehicles can detect its own status (braking, lane change, and acceleration), and also detect vehicle in short range, and understand road conditions (icy, wet, or clear) (Sou, 2013). The safety messaging system connects several technologies and showcase it in an integrated dashboard for motorist and users alike.

While simply marketed and called as safety applications, the safety messaging correlates the data provided from the in-vehicular cameras (Cord and Gimonet, 2014), in-vehicular sonar sensors (Taghvaeeyan and Rajamani, 2012), in-vehicular radar sensors (Liu, Cai, Wang Chen, Gao, Jia, and Li, 2021), in vehicular global positional satellites sensors (Karamete, 2021), and in-vehicular lidar sensors (de Paula Veronese, AuatCheein, Mutz, Oliveira-Santon, Guivant, de Aguiar, Badue, and De Souza, 2021) etc. to build a safety risk data for the motorist at large (Cord & Gimonet, 2014; Taghvaeeyan & Rajamani, 2012; Liu, Cai, Wang Chen, Gao, Jia, & Li, 2021; Karamete, 2021; de Paula Veronese, AuatCheein, Mutz, Oliveira-Santos, Guivant, de-Aguiar, Badue & De Souza,2021).

Preventing accidents was the number one priority for most automotive manufacturers to date, as to why safety systems increased performance for messaging systems, to communicate, collaborate, and connect with other in-vehicular (cars) devices, to naturally develop support for internet of vehicles. Preventing accidents was a tricky calculation that require kinematic status of other vehicles, in intermediate distance (Song, Yang, Fu, Qiu & Wang, 2018). Secondly, convenience application that provided such updates on congestion analysis of traffic required larger effective range. While unknowingly, safety messaging had been engineered to vehicles to protect motorists or end users from any adverse harm, contrary to popularity, systems architects have managed to see that safety messaging is also susceptible to illegal and unauthorized access from unwelcoming elements such as hackers.

Lastly, Systems Architects must realize that neither everything presented by the automotive manufacturers, or automotive theorists were completely sanitized and *re*-tested for performance and safety, nor standardization of technology would be incrementally be a charged concept within the safety messaging system. As unique attack vector and entry-point can ultimately paralyze a good performance of safety messaging, security is nevertheless insecure for VANETs. Exceeding the expectations, systems architects can examine the efforts of the manufacturers, where weaknesses relies to ultimately pave way for automotive vehicle improvements.

In the following chapter, Chapter 3, the primary investigator identified the selected research methodologies, design, and thematic analysis method for the exploratory qualitative study within the topic: *Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers***.** Secondly, within the chapter 3, the selected methodology justified for appropriateness and usage in accordance to the research goals and aims and the overarching research goal for the study. With this basis, the primary investigator identified the correct participants population, population size, and prioritized participants. Data collection instrumentation and procedures would verify the appropriate use of location and estimated length of the research study. Furthermore, data analysis procedures explained in detail to better understand the workaround for the improvement methodologies.

Chapter 3: Methodology, Design and Methods

The purpose of the proposed qualitative study was to explore vehicle security improvements framework (VSIF) in the safety messaging system to protect against external hackers. As generally outlined within the first chapter, the phenomenon is an interdisciplinary area that lies within the area of electrical engineering, communications engineering, and cybersecurity that affects Vehicle Ad Hoc Networks (VANETs), much so known today as Internet of Vehicles (IoV). The safety and security attributes are gathered to formulate improvement methodologies which are examined against stakeholder's practical knowledge, skills, and abilities (KSA) (Armstrong et al., 2020) with using safety messaging system and how it systemically affects the end users (Armstrong et al., 2020). The selected methodology, herein, will follow an over-arching approach to define a selected theme for the safety messaging, such as selecting records of previous implementation problems, analyzing attempts to find deeper meaning of previously defined associated variables, and shifting into thematic analysis to closely examine the data to identify broader aspects of themes.

There were vulnerabilities in the vehicles safety messaging system which are exposed to external hackers. Although the mixed methodology (Terrell, 2012) were encouraged to substantiate the general problem, qualitative methodology (Dowling et al., 2017) modeling were selected to thematized the stakeholder's belief on whether the phenomenon affected them significantly of a positive way, or significantly in a negative way (Terrell, 2012; Dowling et al., 2017). Moreover, the qualitative modeling approach was selected to provide a substantial and impactful meaning to the artifact and the overall pursuit of improvement as a result.

Moreover, some limitations were considered such at the moment, time, and cost model constraints for the research.

The idea of building conceptual framework (Langham et al, 2016) for the study was to build important connections with the suggested topic within the automotive vehicle improvement arena (Langham et al., 2016). The likelihood of interconnectivity between sub-connections on sub-topics and topics were shortly discussed within Chapter 2. In this area, the introduction of the main topics, sub-topics, and generated concepts that linked together from first topic to fifth as they related to the conceptual framework: what are the possible vehicle security improvement framework in the safety messaging system to protect against hacker would also be discussed in Chapter 4. The idea for the conceptual framework was to understand the narrative of where physical, digital, conceptual, or policy-based improvements can affect and potentially decrease system errors, and external attacks from hackers. For visual representation of the conceptual framework, please see Chapter 1, page 5.

Research Questions

This study sought to build improvements to answer to the following research questions:

Q1

What are the possible vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers?

Research Methodology and Design

De Langhe and Schliesser (2017) explained that the importance of exploratory research within the standard applications connected to the capacity to generate more disruptive innovations, for example, electrification, and the internet. The researchers suggested that we must also understand that the explorative research as a research methodology with its ability to produce general purpose technologies, either intellectual, material, and conceptual, that have a large variety of use and multi-purposes: from intellectual and social domains, or can be used in tandem with host of other existing technologies such as social, material, and conceptual (De Langhe & Schliesser, 2017).

In the area of qualitative methodology, the selected type of *exploratory research* would be used by the primary investigator in accordance to the conceptual design of De Langhe and Schliesser's of explorative research to make room for incremental improvement for more exploitative technologies safety messaging system for automotive vehicles. With this effort, vehicle security improvement framework (VSIF) as the improvement feature, and the safety messaging system or basic safety message (BSM) as the exploitative technology that can be set to improve the security posture of the vehicular ad hoc networks (VANETS) which then would be harvested from the semi-structured interviews that would take place with our selected stakeholders, to truly make the research method and philosophy appropriate for the research study.

Interviews. The qualitative study enabled stakeholder interviews (semi-structured; open-ended) (Galleta et al, 2013), in such that selected stakeholders from automotive car manufacturers, communication network providers, and embedded in-car system partners will be approached for an interview process that would consist of open-ended suggestions and answerable questions on the current and posture of the selected topic: Exploring Vehicle

Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers (Galleta et al., 2013). The inclusion criteria set for the selected stakeholder were examined against their practical knowledge, skills, and abilities (KSA) (Armstrong et al., 2020) with using safety messaging system and how it systemically affects the end users (Armstrong et al., 2020).

Galleta et al. (2013) expressed that the key to effective interviewing is the researcher's attention to the participant's narrative as it is unfolding (Galleta et al. 2013). The participant's time would be used wisely to construct an improvements methodology about the selected industrial situation. The market vectors would be analyzed and correlated to the current security approach and methodologies used in the automotive informatics security, where current problems can be discussed.

Population, Sample, and Participant Recruitment

Population. The population of the study was purposefully selected based on their level of importance within the field of Internet of Vehicles (IoV), primarily the stakeholders within the vehicle ad hoc networks (VANETS), automotive informatics security that can be leveraged for their knowledge, skills, and abilities (KSA) particularly the one that affects secure automotive systems: (a) embedded system providers (Oh et al., 2005), (b) automotive electronics organization (McHugh, 1998), (c) cloud service providers (Kang et al., 2014), and (d) the vehicular participants (Kim et al., 2019) as they affect the integration of safety messaging system, or basic safety message (BSM) (Oh et al., 2005; McHugh, 1998; Kang et al., 2014; Kim et al., 2019). The population for the study will therefore include automobile manufacturers, embedded automotive system providers, automotive organizations, next generation connected data providers that can relate to the explorative approach that embodies vehicle security improvement frameworks within the safety messaging system.

The research explored specific improvement framework (Temoponi, 2005) that might arise within vehicular communication networks as it pertains to safety messaging, vehicular architecture as it pertains to safety messaging, and safety algorithm issues as it pertains to safety messaging (Temoponi, 2005). Basic Messaging Concepts are to be asked if proper integration of channels have occurred. Areas that pertains to messages, pipes and filters, routing technology, transformation, and endpoints may be asked for within the desired thematic analysis questionnaire. Temponi et al. (2005) notes that continuous improvement is one of the core values of quality management (QM), which is a people-focused system through performance by stressing learning and adaptation as keys to the success (Deming, 1994; Evans and Lindsay, 2001; Tamponi, 2005).

The participants of the study knowing as technology leaders, technology managers, and network and security system administrator, would have greater understanding of safety messaging system integration within vehicle networks. Secondly, realizing that the selected participants have verifiable assumptions through industry set standards, protocols, and practitioner based learnings versus variations from theoretical constructs that differs from improvements in terms of system security and safety of hardware and software feature, as they affect the drivers of today, mostly our end-users, certainly would be helpful in determining the future of safety and security of most safety messaging system, or basic safety message (BSM).

Population and Sample Size. Carlier (2021) stated that the motor vehicle and parts dealers in the United States have a population size of 2 million employees on their payrolls in June of 2021 (Carlier, 2021). Out of the motor vehicle and parts dealers, the number of motor vehicles and parts manufacturing employees amounted to roughly 873,000 people in June of 2021, up from around 850,000 the same month a year earlier. From those parts manufacturing population, the study admitted about 6 subject matter experts available to do the study, as our sample size who has knowledge, skills, and abilities (KSA) in vehicle ad hoc networks implementation, particularly as it related to secure systems and safety messaging system workarounds. The esteemed participants are part of the technical stakeholders within the parts manufacturing sector that implements electrical, mechanical, vehicular, and security frameworks for the automotive manufacturing sectors. Handpicking a small sample size allowed for personalized learning from the subject matter experts that provided the study with very distinct and accurate summary of the security postures within automotive practice, though qualitative semi-structured interviews through interpretations of codes until reaching saturation.

This upward trend in the employment were likely to continue, as the projected automobile demand in the United States were higher than in the year 2020, post pandemic demand. The sample size for the study qualified around 10 subject matter experts, but only 6 subject matter experts remained available for the study as participant respondent for the explorative approach within the thesis: Exploring Vehicle Security Improvements Frameworks in the Safety Messaging System to Protect Against External Hackers. Spencer et al. (2003)

suggested that sample adequacy in qualitative study pertains to the appropriateness of the sample composition and size. It is a very important segment to note the right number of participants in a research study, for consideration in evaluations of the quality and trustworthiness of much qualitative research (Spencer, Ritchie, Lewis, and Dillon, 2003). As we employed qualitative strategies for the study, explorative approach will not as much require the importance of having plenty of participants to do a semi-structured interview, but therefore acquire the correct participants to verify and reach saturation at the end of the semi-structured interview. In this research, the primary investigator will model elicitation process to include automobile manufacturers, embedded automotive system providers, automotive organizations, next generation connected network data providers, and motorists up to about around 10 qualifiable participants to relate to the explorative approach that embodies improvements in safety messaging system.

Prioritized Participants. The prioritized participants for the study leveraged a holistic outcome, prioritize highly skilled participants, and sampling preference would be given to the following roles:

Chief Information Officer – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Chief Information Security Officer – (Internet of Vehicles, Embedded Systems, Safety Messaging Systems)

Systems Architect – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Systems Manager – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Configuration Manager – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Hardware Engineer – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Software Engineer – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Security Analyst – (Internet of Vehicles, Embedded Systems, Safety Messaging System)

Data Collection Instrumentation and Procedures

Location. The qualitative study conducted on a high demand face-to-face (in-virtual audio/visual) interview in effect, to capture a much broader audience of the U.S. automotive market, in response to validate the explorative approach. More likely, the qualitative research will be conducted, in no particular order: (a) semi-structured interview, and (b) web-based meetings. The qualitative research study requires a few steps to gather participants in the location, where the primary investigator had provided a participation invitation letter and letter of permission and is required to be approved by the authorized decision maker to use participants within the field of automotive manufacturing. There, also requires an informed consent where consent forms were signed for the complete participation process within the virtual Zoom interview, Skype for Business, or Citrix interview, whatever is available for the participant. Also, a set of interview guide, interview questions, and interview protocol that will serve as guidance for both the primary investigator and the participants have to be exchanged.

Estimated Length. The length of each semi-structured interview for the study came out to be approximately at least 50-minute time frame for the semi-structured interview for each participant. The overall capture of the study should be determined according to the demand, logistic, and research cost consideration. The overall value, of the responses gathered, were tested to validate research performance and reliability of results generated from qualitative analyses. The qualitative methodology came in three phases for the research. The qualitative phase wss staggered in three phases in a way that if one task is about to end another one is also beginning in the process. For Phase 1: (a) identify the problem, (b) review the literature, and (c) clarify the problem. For Phase 2: (d) clearly define the terms and concepts, (e) define the population, and (f) develop qualitative research instrumentation plan. For Phase 3, (g) collect qualitative data, and (h) analyze the qualitative data.

The interview consisted of 10 semi-structured interview questions that aimed for conversational aspects of practice which goes through the aspects of improvement methodologies within safety messaging system. This conversation held by the primary investigator against the research participants used a semi-structured approach to allow for additional probing that would allow for some level of flexibility within the elicitation process. the aim is to conduct the interview with stakeholders of newer built vehicles post 2019 and later who had direct understanding of safety messaging systems, embedded controls, and in-vehicular technologies. A respondent was defined as a person who had used and tested the in-vehicular safety messaging system. Research participants (respondent) are given at least 50 minutes time frame for the semi-structured interview, per participant candidate, anonymously for participation confidence. The research participants are given enough time at their disposal to participate in the research project. The research participants will not be coerced, time-limited, and answer questions unwillingly. After completion, only the required 8 interview results are to be included in the analysis.

The data collection for the semi-structured interview consisted of the identification of 6 subject matter experts that met the criteria as a participant respondents on the automotive safety messaging system, or basic messaging system (BSM) survey that comprise of highly selected participant stakeholders, customers, and end users creating effective relationship within the Internet of Vehicle environment. Though conversations in-virtual meetings don't flow as naturally as in-person groups, especially when the group is large. Ramachandran (2021) documented that the reasons for not being effective with large groups is that we tend to have cognitive overload during meetings, based on too much eye contact, and not enough non-verbal communications. The more people included in the virtual meeting, the more challenging the dynamic of collaboration becomes (Ramachandran, 2021). Secondly, with having the qualified 6 research respondents, taking the interview format would not be as difficult and time consuming for the primary investigator.

Data Analysis Procedures

With observation, the participant observer (primary investigator) may be able to direct themselves within the shoes of the human subjects, or rather, see a different light on how a particular common practice, or central phenomenon is held, neither possible if not extended, nor experienced by themselves, in a controlled setup environment. In light, data gathered within the process had some benefits reap only by those who understood and trusted the process of exploratory study, as this method far rather outweighs any series of qualitative research pitfalls by default. In this discussion, we'll explore two observational methods preferably used for qualitative research – and how it can be directed to any qualitative research, as a whole.

Apart from data collection techniques, such as the semi-structured interview, probing was a processes which became so critical to enrich the context, as general understanding of claims and assumption provided by the subject matter experts expressed contextual layers of situation, and see the angles in which the qualitative data is perpetuated to lead. The research added probing thereafter each question was observed and were contrasted to the particular central phenomenon. In this approach, understanding of the current traditions and models of qualitative study on the phenomenon Exploring Vehicle Security Improvements Framework in the Safety Messaging System to Protect Against Hackers were validated through the rich aspects of interview technique. The data collection techniques especially probing procedure is a carefully manicured procedure to highlight and focus on techniques presented by the participants.

Interviews [web based]. In this process, the primary investigator (researcher) argued that the primitive role of web based audio-visual call interview would still secure the true feelings, emotions, and infatuation of a human subject towards the common practice, or the central phenomenon. The sample size for the study was drawn largely from Intelligence Vehicle Network forums and journal members, as well as Auto Engineering Forum from NEC. The sample size for the study will also draw from research membership only members ORCID – Connecting Research and Researchers, and ResearchGate research members from the field of Internet of Vehicles.

The semi-structured interview and study took place on-line and recorded live via the following communication tools: Zoom (www.zoom.us), Microsoft Skype for Business (www.skype.com), Cisco Webex Meetings (www.webex.com/conference-call.html), or Citrix GoToMeeting (www.citrix.com) on a virtual desktop infrastructure (VDI), with the interview to also interpret the sentiment of the highly skilled engineers and consultants. The set timeframe from the study is 50 minutes for the semi-structured interview to answer the question that is relative to the strategies to answer the thesis question: What are the possible vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers? The host communication solutions Zoom and Skype limits meeting up to 45-minute time frame.

The interview transcript for the study required the use of ATLAS.ti (www.atlasti.com) and NVivo (www.qsrinternational.com) Qualitative Data Analysis software. With the on-line interview, the observer/ primary investigator will have to understand the subtle vocal cues of the respondent, whether the respondent is mad, happy, elated, euphoric and etc. After conducting the semi-structured interview, the interview transcripts will be analyzed through with the use of the thematic content analysis technique. One would need to understand intonation, messaging, and delivery to understand the full context, as well. After transcription is commenced, the transcript shall be reviewed by the participant for review and confirmation.

Thematic Analysis. Nowell Lorelli et al. (2017) expressed that the process of conducting a thematic analysis is illustrated through the presentation of an auditable decision trail,guiding interpreting and representing textual data (Nowell Lorelli, Norris, White, & Moules,2017).

Thematic Analysis procedure is where the researcher will present clear themes generated according to the answers selected on the interviews. Steps involved include the following (a) familiarizing with data, (b) generating initial codes, (c) organization of codes (combine similar), (d) searching for themes, (e) reviewing themes, and (f) defining and namingthemes.

Reliability of Coding Process. Miles et al. (2014) expressed that codes are labels that assign symbolic meaning to the descriptive or inferential information compiled during a study. Codes are usually attached to data "chunks" of varying size and can take the form of a straightforward, descriptive labels or more evocative, in the likes of a complex metaphor (Miles, Huberman, & Saldana, 2014). Secondly, the primary investigator (researcher) further assume that the basic, raw data (recordings, field notes) must be processed before they are available for analysis.

In this segment, the explorative approach overall quality is sanitized, collected, and or de-coded. The process can be somewhat significant to the overall conclusions of storylines, and somewhat pivot thinking for a particular phenomenon. In this analysis model, we gather artifacts presented by participants from our study to *describe* and *code* thought ability, process, misfortunes, or results returned by the selected participants of study.

Techniques of Coding Process. Saldana (2015) attested that the following techniques from *the coding manual for qualitative researchers* can be formatted to demystify qualitative coding process within the study, which brings about different coding types, examples, and exercises for practitioners of qualitative inquiry (Saldana, 2015). The following coding techniques, also see Figure 3, p. 59, will be used for the study of *Exploring Vehicle Security Improvement Frameworks in the Safety Messaging System to Protect Against External Hackers*:

a) **Pre-coding on passage** – Boyatzis (1998) expressed the process of pre-coding requires circling,highlighting,bolding,underliningorcoloringsignificantparticipationquotesand passages that are useful for the study (Boyatzis,1998).

b) **Jotting the codes on passage** – Liamputtong and Ezzy (2005) suggested that a researcher can collect valuable, sensitive information that can be coded. When you are writing field notes, or transcribing interviews, jotting the preliminary words and or phrases for codes to transcripts, to documents, to analytic memo help in referencingthe preliminary investigator's thoughts into document. Secondly, jottings within the code should in any way be placed on bracketed, capitalized, italicized, and bolded formats (Liamputtong & Ezzy, 2005, p.270-273).

c) **Questioning the codes on passage** – Auerbach and Silverstein (2003) cited that the a researcher must keep a copy of concerns, theoretical framework, central research question, goals of the study and other major issues within the interview to keepfocused because such itinerary focuses the coding decisions (Auerbach & Silverstein, 2003, p. 44).

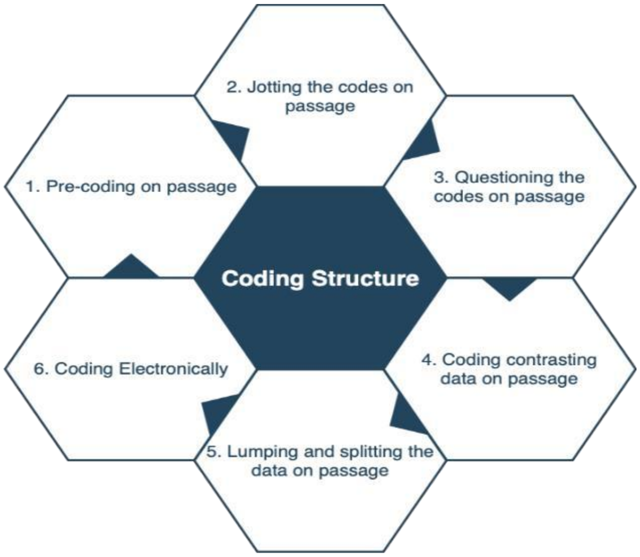
d) **Coding contrasting data on passage** – Bazeley (2007) conditioned that if working with multiple participants, it's very important to code one participant data first, then progress with the second participant. You might find that the after the second or third participant data, the coding might influence you and affect your recording process.The reasoning as to why there requires less participants in the coding technique, because coding requires a more robust analysis and techniques. This is called consequent coding. The same may be true with interview transcript, then day's field notes, then to a document. Bazeley (2007) recommended that the second document must at least contrast the preliminary document, to include potential for variety of concepts in the process (Bazeley, 2007, p. 61).

e) **Lumping and splitting the data on passage** – Saldana (2015) noticed that lumping requires less coding, and that one In Vivo Code (NVivo) can be applied to capture and represent the essence of at least 145-word excerpt, and many more, which is can bea brush stroke presentation called holistic coding. This is suggestive of lumper coding, while the opposite situation may be called as a splitter coding, whereby many data is split into smaller and individual moments. (Saldana,2015).

f) **Coding electronically** – Richard and Morse (2007) suggested after doing the coding one byone,fromhardcoding,andhavedevelopedabasicunderstandingoffundamentalsof qualitative content analysis, apply experiential knowledge based on Computer-assisted qualitative data analysis software (CAQDAS) (Richard & Morse, 2007). With NVivo, the software allows to handle documents in rich text format, enabling the use of supplemental cosmetic coding devices such as colored fonts, bolding, and italicizingyour data (Lewins & Silver, 2007, p.61). Page 54 of Chapter 3 suggest the use of ATLAS.ti and NVivosoftware.

Figure 3

Collective Excerpt of Coding Process from The Coding Manual for Qualitative Researchers made as Qualitative Coding Structure


2. Jotting the codes on passage
1. Pre-coding on passage
3. Questioning the codes on passage
Coding Structure
6. Coding Electronically
4. Coding contrasting data on passage
5. Lumping and splitting the data on passage

Note. From the Coding Manual for Qualitative Researchers, by J. Saldana, 2013. Pre-coding on passage technique, by Sapsford and Jupp, 2006. Jotting the codes on passage technique, by J. Saldana, 2013. Questioning the codes on passage technique, by Auerbach and Silverstein, 2003. Coding contrasting data on passage technique, by Bazeley, 2007. Lumping and splitting the data on passage technique, by J. Saldana, 2015. Coding electronically technique, by Richard and Morse, 2007.

Trustworthiness

According to Elo et al. (2014), the trustworthiness of qualitative content analysis was often presented by using terms such as credibility, dependability, conformability, transferability, and authenticity (Elo et al., 2014). Research among security engineering must conveniently include integrity, trust, and responsibility. The foundation of research should be built upon trust between the researcher and the subject (selected population). Researcher must be careful in ensuring that this trust is never to be broken between both parties. Analyzed research data must be truthful, by any nature, to fulfill our obligations as a researcher. It's fundamental that we shared our results to our sponsors or subjects as part of our responsibility and accountability for our human subjects, whether we're including experimentation process, or eliciting important data. It was tangible to continue our work in producing ethical products and processes for the enrichment of the body of knowledge, and future research endeavors.

According to Lincoln and Guba (1985), trustworthiness was met by following the four alternatives for assessing trustworthiness in qualitative data research. The alternatives suggest the following terms of credibility, dependability, conformability, and transferability are the evaluating factor in terms of trustworthiness.

a) **Credibility** – Polit and Beck (2012) suggested that credibility deals with the focus on the research and refers to the confidence in how well the data address theintended focus (Polit & Beck, 2012).

b) **Transferability** – Polit and Beck (2012) expanded that transferability refers tothe potential for extrapolation. It relies on the reasoning that findings can be generalized or transferred to other settings orgroups.

c) **Dependability** – Polit and Beck (2012) expounded that dependability refers to the stability of data over time and under differentconditions.

d) **Confirmability** – Polit and Beck (2012) agreed that conformability refers to the objectivity, that is, the potential for congruence between two or moreindependent people about the data's accuracy, relevance, or meaning (Lincoln & Guba, 1985; Polit & Beck, 2012).

Ethical Assurances

According to Kenneally et al. (2015), *ethics-by-design* were important in the field of cyber security research. The authors expanded on the following: (a) educate participants about underlying ethics principles and applications; (b) discuss ethical frameworks and how they were applied across the various stakeholders and respective communities who are involved; (c) impart recommendations about how ethical frameworks can be used to inform policymakers in evaluating the ethical underpinnings of critical policy decisions; (d) explore cyber security research ethics techniques, tools, standards, and practices, and (e) discuss specific case vignettes and explore ethical implications of common research problems (Kenneally et al., 2015). By assuring ethics would become a central point of the qualitative research, a disciplined approach to minimize risk to human subjects, may ultimately provide potential security improvement and benefits that is requested from the automotive manufacturer and SMEs during the semi-structured interviews without imparting any types of indifference, hesitations, and fear toward the study.

In security engineering, not only the goal supposedly were to secure digital assets (Son et al., 2019), critical assets (Srivasan et al., 2013), and secondary assets (Pasquale et al., 2012) of the enterprise, but also impart recommendations much known as improvement that would affect each end user's environment, hence improvement was required, not only necessary, whether that be in the assigned department, or the organization itself (Son et al., 2019;

Srivasan et al., 2013; Pasquale et al., 2012). Much work was looked upon within security implications (Davis 2005), where vast amount of research rich projections can suffice a new product, policy, or security framework in a national infrastructure, particularly Vehicular Ad Hoc Networks (VANETs) (Davis, 2005). The researcher found that it was important to embed ethics-by-design (Ibiricu et al., 2020) in any elicitation semi-structured interviews, in any cyber security research, as part of any product or framework engineering initiatives (Ibiricu et al., 2020). As it is an emerging area, it will be great for future engineering researchers to make ethics as a foundation in which we create, amend, use our policy, framework, or generate products, in respect to the desired population.

Chapter Summary

Chapter 3 implemented the qualitative research where qualitative design was implemented to broadly showcase sentiments from participants and extract improvement qualifications. The chapter also discussed the research methodology and design where interview (semi-structured) efforts were taken into consideration for the human subjects. The conceptual framework and questions were revisited to align with the styling of the of data collection procedures, much throughout that solidified the use of virtual face-to-face interviews and enacted several communication platforms for participants. Coding process and techniques were also discussed as to how it will verify analysis for the following chapter.

The confidentiality, integrity, and availability of information transmitted to vehicular ad hoc networks (VANETS) that collects data within the safety messaging system, or the basic safety messaging system (BSM) were shortly becoming the automotive manufacturer's problem. With an interest to ensure embedded systems, telematics devices, and automotive data are protected, automotive organization's must realize either how effective or how flawed its security posture against its enemy's attacks and implementation of automotive systems itself. New technologies, such as assistive technologies, artificially intelligent systems, vehicular communications, and possibly in-vehicle application all sort to be exposed from the dangers of an impending attack—whether it be state sponsored (Giles et al., 2019), service high-jacks (Alkadi et al., 2020), or malware intrusion (Katkar et al., 2021) to debilitate an operator's ability to navigate the vehicle singlehandedly (Giles et al., 2019; Alkadi et al., 2020; Katkar et al.,2021). Moreover, should crises continue, a significant effort from the automotive industry, its partners, and data providers should provide mitigation efforts to advert risks that may endanger the registered motorist (Amin et al., 2015). The literature to be reviewed discusses themes of confidentiality, integrity, and availability and how the integral structure affect production and end-user atlarge.

Chapter 4: Findings

The purpose of the proposed qualitative study was to explore the vehicle security improvements framework (VSIF) in the safety messaging system to protect against external hackers. The 6 subject matter experts and participant respondents come from various backgrounds from network operations, security operations, federal cybersecurity contracting, transit authority organizations that work within the automotive sector. Participation merits both technical and non-technical backgrounds in their approach to securing safety messaging systems in either use of production vehicle, fleet buses, and railroad systems.

Description of the Study Sample

The participants for the qualitative research study included network professionals, supply chain cloud software professionals, transit authority executives, and cybersecurity professionals working directly and indirectly within the vehicle ad hoc network organizations. Each of the participants were contacted through LinkedIn, ResearchGate, NEC, and ORCID messaging through the immense power of social media. As each of the participants agreed to be part of the qualitative study utilizing semi-structured interviews, the investigator sent interview letters for each participant asking for individual availability and schedule. The participants for the qualitative research study have different role composition and breakdown within the organization, some were technical, while others were non-technical giving them different subgroups within the research. Nevertheless, the opportunity of shared knowledge within cybersecurity, safety, and privacy were very evident in protecting private vehicle and fleet buses. Some of the participants were in the management, others held executive level positions within the public sector, while other specified engineering and analysis positions requiring them to be broken down into subgroups. There were 10 qualified participants for the study that were accepted the invitation. Meanwhile, only 6 participants showed to actual semi-structured face-to-face interview (video call). All of the qualified participants agreed willingly for the semi-structured interview. The population group comes from about the motor vehicle and parts manufacturing population employed as of 2021 to about 870,000 of which an anticipated size of the target group of about 4,000 are qualified, and an estimated 10 were selected, but availability of only 6 SMEs came.

The chapter four represented the thematic analysis within the semi-structured interview with esteemed 6 subject matter experts with knowledge, skills, and abilities within the Vehicle Ad Hoc Network industry. The semi-structured interview underwent 10 questions that required the participants to provide descriptive details within their timeline at their local transit authority agency or automotive organization relating to their security practices. The knowledge of each participant were most evident within their answers given an approximate of 55-minute timeframe to gather all questions and answers for the interview together withcompleted

probe questions to uncover layers of depth within answers. Thematic analysis was a notable choice for the data analysis, since the answers from each human participants were subjective to their unique practices, thus given a high priority, detailed based upon their collective experiences, and mixture of subjective techniques and preferences within the automotive industry. Similarly, specific themes surfaced through the help of ATLAS.ti and the NVivo (www.qsrinternational.com) qualitative analysis software.

The use of the thematic analysis presented significant themes that were uncovered from useful words and repetitive phrases better known as excerpts that emit patterns, as to procedural behaviors, and nuances that are unique to one's practice. Additionally, these repetitive words and phrases that appear to have the same meaning are highlighted and made as theme. In this qualitative process, the answers were coded to extrapolate subsets of themes and sub-themes and were arranged to order of significance and importance to the industry.

Since the research were mainly a qualitative process, the significance from each theme(s) would not be tested and presented, as it is not a quantitative procedure. The selection of the thematic analysis was fitting for the qualitative research as it provided and casted a clear picture of the current state of affairs within the vehicle ad hoc network arena. The semi-structured interviews allowed for a variety of responses from participants giving texture, highlighting the general phenomenon, and proving the importance of the relative subject. The order of participant interviews was based upon availability of each selected participant respondents.

Since the data was in the form of an audio file, the software had to convert and transcribe the file to read through the answers from the semi-structured interview. Reading through the transcription then required the need for the creation of codes. These codes were helpful in selecting and highlighting the themes that were further of significant importance. These codes acted as a decoder to showcase which excerpts were in relative increasing importance.

The geographic locations of the participants within the qualitative data analysis were spread across the continental United States. One participant came from the State of Maryland, two participants came from the Commonwealth of Virginia, two participants came from the State of Illinois, and one participant came from the State of New York. Due to disproportionate geographic disparities, remote sessions were used to effectively manage time of respondents in such that Zoom Audio calls were utilized for most of the semi-structured interviews. The qualitative interview was done from the beginning of September 2022 until around the end of September 2022. The subject matter experts that qualified as participants were all voluntary and was not hurt during the process of interview.

Results

Participant Core Mission in Table 1 represented the participant frequency and sample distribution related to each core mission involved within vehicle ad hoc networks. Apparent in the distribution index were the participants involved in the core mission that relates to engineering communications, computer networks, and cybersecurity.

Participant Organization Size in Table 1 represented the frequency and sample distribution of each participants related to organization size. Within the returned demographic questions, there were a significant population that is employed within mid-size organizations with 50,000 employees that work for the automotive sector.

Participant Expertise in Table 1 represented the frequency and sample distribution of each participants related to expertise. It also represents the frequency and sample distribution of each participant related to each role that were required for the semi-structured interview.

The participants were subject matter experts within the vehicle ad hoc network industry. The role makeup of the participants showcased a larger distribution with roles as cybersecurity manager and chief executive officer within the automotive manufacturing and transit authority distribution.

Participant Experience in Table 1 represented the frequency and sample distribution of each participants related to their experience in years. Within the returned demographic questions, there were a balanced return between who have about 10-15 years cumulative experiences, and 5-10 years cumulative experience, whereas the 1-5 years cumulative experience, and 15-20 years of cumulative experience have relatively lower respondents within the automotive or transportation sector.

Participant Education in Table 1 represented the frequency and sample distribution of each participants related to their highest educational attainment. Within the returned demographic questions, there have been a significant rise to both Bachelor's and Master's attained credentials before assuming role within automotive or transportation sector.

Participant Field of Study in Table 1 represented the frequency and sample distribution of each participants related to their field of study. Within the returned demographic questions, there have been a significant return to Technology credentialed participants within the automotive or transportation sector.

Table 1

Distribution of Participants within Vehicle ad hoc Networks Study

Participant Core Mission	*n*	Relative
Automotive	1	.2
Manufacturing	1	.2
Supply Chain	1	.2
Engineering Communications, Computer Networks, Cybersecurity	3	.4
Total	**6**	**1**
Participant Org. Size	*n*	Relative
0-100	0	0
100-500	0	0
500-1,000	1	.2
1,000-10,000	1	.2
10,000-50,000	4	.6
50,000-100,000	0	0
100,000+	0	0
Total	**6**	**1**
Participant Expertise	*n*	Relative
Security Analyst	1	.1
Software Engineer	1	.1
Security Manager	2	.4
Chief Executive Officer	2	.4
Total	**6**	**1**
Participant Experience	*n*	Relative
1-5 Years	1	.1
5-10 Years	2	.4
10-15 Years	2	.4
15-20 Years	1	.1
20-25 Years	0	0
25-30 Years	0	0
Total	**6**	**1**
Participant Education	*n*	Relative
A.S., A.A.	1	.2
B.S., B.A., B.E.	2	.4
M.S., M.A., M.E., M.B.A.	3	.4
Ph.D., D.Eng, D.Sc., Ed.D., D.C.S., D.A.	0	0
Total	**6**	**1**
Participant Field of Study	*n*	Relative
Science	1	.2

Technology	4	.6
Engineering	1	.2
Mathematics	0	0
Total	**6**	**1**

**n*=6

Procedures for Qualitative Data Analysis

The interviews were coded with Atlas.ti and NVivo qualitative research software to conduct initial coding, and themes, and categories for the study. Much of the coding process that occurred for the Atlas.ti would provide a revealing trend about a particular theme for each of the questions provided for each of the participant respondents. Some questions would be seen and taken by the system as a more significantly pronounced subject qualifying into a theme. Reoccurrence of themes are also possible for some of the questions and the answers involved and would definitely count into a frequency.

The procedure to analyzing the qualitative data are the following:

1. Familiarize with audiotranscript;
2. Transcription of audiofiles;
3. Creation ofcodes;
4. Highlighting interestingexcerpts;
5. Application of new appropriatecodes
6. Collating codes with supportingexcerpts;
7. Grouping codes asthemes;
8. Evaluation and revision ofthemes
9. Presentation ofthemes

Phase 1: Familiarize with Audio Transcript

In this phase, I had to manually collect audio transcription through a recording. The recording occurred through Zoom Audio, to initially take proof from respondents about the given phenomenon. In Phase 1, I had to manually override from the original 45-minute limit of Zoom session to 55-minute interview to give each respondents a chance to talk and explain events within each of the questions. The respondents were given a chance to back out or talk if necessary, within their own free will, as we undergo the process of recording.

Phase 2: Transcription of Audio Files

In Phase 2, I had to manually transcription the set of local audio files saved from the interview within a Microsoft Word processor one by one from each selected participant respondents to initially tabulate responses from each of the semi-structured interview Zoom Audio recording. The transcription would occur later after all the audio files were reviewed and provided file names, anonymized participant, and reviewed for quality assurance. The transcription served as a tabulated response from the interview questions that would later be used for initial coding. Worded transcription had to be saved as a .txt file for the Atlas.ti to perform coding and analysis

Phase 3: Creation of Codes

In Phase 3, I had to upload transcript to add documents > add file. To be able to create the code, I had to grab a text from the simulated transcription file and pulled with left hand side of the mouse to highlight, right click on the text, and select to perform InVivo coding for the file. When the specific word or phrase has been highlighted by software, it would capture the word or phrase and simulate it into the split screen and add a code for the selected text.

Phase 4: Highlighting Interesting Excerpts or Extracts

In Phase 4, I had to highlight all interesting excerpts from the all questions. All questions from question 1 through 10 including the probe questions, too, if necessary. The highlighted excerpts were then highlighted, right clicked, and selected for InVivo coding on file. The phase was performed to all responses from the semi-structured interview. So, manually uploading transcription is necessary.

Phase 5: Application of New Appropriate Code

In Phase 5, I had to create new appropriate codes that stick out for the phenomenon. The new codes were tabulated and highlighted through the split simulation screen. The codes would be numbered according and highlighted to the multiple text documents that were uploaded within the Atlas.ti qualitative research software. Reoccurrence of codes from the multiple text documents would occur as frequency. In the explore pane, under codes, the application of new codes would be highlighted and arranged by occurrence. Colors could be used to generate variations in coding.

Phase 6: Collating Codes with Supporting Excerpts

In Phase 6, the codes had to be linked with supporting excerpts. In this situation, multiple documents have to be uploaded at ones for all individual semi-structured interviews taken and transcribed within the Microsoft Word .txt file documents to be scanned by the Atlas.ti qualitative research software. Condensing text rich information requires that the use of 'add code to quotation' where if a coded word or phrases have already been selected, it would appear within the selection.

Phase 7: Grouping Codes as Theme

In Phase 7, the group of reoccurring codes would be processed as themes. These group of reoccurring codes were collected to justify the promotion of a given theme, for presentation as top themes. These would allow the data to be much more robust and coherent, rather than be condense and confusing to many readers alike looking at the research.

Phase 8: Evaluation and Revision of Themes

In Phase 8, The evaluation procedure would collect coded themes and check for validity. The revision to the collected coded themes are to be the selected, themes are selected and qualified, those subjects that have high or popular demand, reoccurring hot topic key words and key phrases, notable excerpts, and continuous sentiments of the participant respondent are to be given prioritization and revised to belong to the top themes and would be promoted on top of the themes. Later, those with the highest reoccurrence will end up becoming the key themes to be presented as a qualitative result.

Phase 9: Presentation of Themes

In Phase 9, the presentation of themes would be provided together with the associated excerpts and the answers from the selected participant respondents. Only top three themes are selected, per Colorado Technical University guidance. The top three themes would commensurate the thematic framework for Vehicle Security Improvement Framework.

Discussion of Study Findings

There were at least 10 questions and additional probe questions given to each participant involved in the qualitative study. The participants were given 55-minute to finish the semi-structured interview. Axial transcription had also been collected prior to determining the selected themes for each answer. The questions that were used for the collection of themes were the following:

1. Briefly describe your role (automotive, manufacturing, supply chain, engineering, cybersecurity, network) as it relates to automotive manufacturer and security assessment (ifappropriate).
   a. *Probe question*: How are you involved in the teaching, learning, and security assessmenthere?
   b. *Probe question*: How did you getinvolved?
2. What is the strategy at this institution for improving security learning, andsecurity assessment to prevent undesirable external attacks tonetwork?
   a. *Probe question*: Is itworking?
   b. *Probe* question: Why or whynot?
3. What is the biggest misconception about vehicle security that is apparent intoday's automotive manufacturing?
   a. *Probe question*: Why do you thinkso?
4. What are some of the major challenges your department faces in attempting tochange security learning, and security assessment practices in safety messagingsystems?
5. What element are you willing to give up for a good connected network onvehicles?

6. How far are you willing to go as a cybersecurity team to be protected againsthackers?
7. What are the secure standards you use for vehicle ad hocnetworks?
8. What are the possible vehicle security improvement framework in the safety messaging system to protect against externalhackers?
   a. *Probe question*: How can barriers be overcome for safety messagingsystem?
   b. *Probe question*: How can opportunities be maximized for safety messagingsystem?
9. What kind of resistance did you and your colleagues get during security improvement meetings?
   a. *Probe question*: How often do you get this as aresult?
10. To what extent are security improvement-related activities evaluated at your institution and yourdepartment?
    a. *Probe question*: How is security improvementrewarded?

The divide between secure standard usage vary from organization to organization, particularly if an organization is in the private sector, it had a rather different production, nonfunctional, and functional requirement as data distribution is provided for the consumer facing driver-user. So, secure standards were entity specific for Network and Cloud providers. While organization in the public space specifically that came from the transportation sector do abide by federal guidelines chartered by the U.S. Government.

These differing conceptualizations of vehicle safety improvement framework (VSIF) clearly influences how the automotive groups, network of cloud providers, and transit authority organized to protect their safety messaging to the public, whereby public sector organizations such as a local transit authority may have a more pronounced issue in terms of a cyberattack within safety systems if it can cripple the day to day fleet operations.

These participants came from various institutions who were separated in research subgroups were very well aware of an increasing risk of an attack to their institutions cyber systems particularly embroiling within the safety messaging systems to destabilize communication between manufacturer and network provider towards driver-user of the vehicle. As I uncovered the persistent situation, safety messaging system not only had become an integration priority for the many participant institution's communication planning, but it had become one of the manufacturer's critical asset that requires protection. To the general public's interest, safety messaging system was a way for manufacturers to elevate event response guidance, critical and safety hazard communication, vehicle performance, and communicate vehicle traffic health. It was rather a way to instill a peaceful mind to all motorist, as it is part of their communication asset giving them the ability to communicate how soft or hard an critical event is supposed to being the auto manufacturer, network or cloud providers, to the driver and passenger aboard of a vehicle.

Moreover, the importance of a secure implemented systems had never been more recognized as safety from intrusion is also an ongoing threat vector from drivers unable to operate due to lapses in communication and being unable to connect important messages from system health of the vehicle towards the passenger. Disabling such connection also eliminated the ability to transport critical event response initiated from network providers to the rolling vehicle.

Interview Question 1, Theme 1: Visiting security protocols and security framework annually. In an open-ended response, participants felt highly about the visiting security protocols and security procedure annually to protect network against from any hackers, P02 (Executive Director for Safety, Security, and Quality Assurance) is compelled to act with full force of his department:

> *I'm also a Cyber Coordinator which is pretty much the liaison between the Department of Homeland Security, Transportation Security Administration, and our agency [Potomac and Rappahannock Transportation Commission] in our region. I essentially handle and look at potential threat coming from overseas and into the cyberspace. Is there any new threats? And then I go back and give it to my agency and put down protocols together and procedures in protecting the networks.*

Interview Question 1a, Theme 1: Cyber projects within vehicle ad hoc networks should focus on data privacy. Meanwhile, in the open-ended response, participants felt that cyber projects regarding about vehicle ad hoc networks should focus more about privacy compliance and should come as a top priority for auto manufacturing organization, especially those that operate in region specific areas, and P03 (Product and Program Manager for SAS Institute) that handles data operation for an automotive group client in Europe says privacy management is key aspect:

> *But I work for the R&D side of the company for the projects I manage or oversee, there are some level of security compliance that we need to go through primarily GDPR for Europe and that is the main security compliance for personal data compliance that we*

> *tend to go through as a part of our regular cadence for validating software before they go public.*

Interview Question 2, Theme 1: Distributed teams across safety messaging system. Additionally, in an open-ended response, participants felt highly distributed and collaborated teams with various roles across all domains are extremely helpful in curbing vulnerable areas within safety messaging systems, P01 (Network and Security Operation Engineer for a top cybersecurity group) mentions:

> *In terms of learning management, broken down to levels and roles, we use different sets of guidelines to secure the networks. We use organizational security controls to prevent the likelihood of an adversarial attack and reconfigure our assessment plan if necessary.*

Interview Question 2, Theme 2: Cyberattacks in safety messaging systems are both public and private sector problem. In the open-ended responses, participants described how debilitating a cyberattack could be both a problem between private sector and public sector especially in the operation domain. However, P02 (Executive Director for Safety, Security, and Quality Assurance) mentioned that the security assessment is done more frequently for their organization:

> *We basically do four assessments. Monthly, quarterly, annually. Based on that, we look at it and say okay we have to have a refresher training on this and the other. We have annual refresher training on every single aspect of cyber security, physical security, bomb threat analysis, we have that annually. But, in between that, we find something in a month's time, we may do an emergency training in between that annual training*

Interview Question 2, Theme 3: Automotive and public transit groups require periodic use of vulnerability and risk assessment program. In the open-ended responses, participants felt the impact of an impending cyberattack situation and requires periodic use of vulnerability and risk assessment programs and P02 (Executive Director for Safety, Security, and Quality Assurance) mentioned that the likelihood of a cyberattack could surface into any fleet circulator buses, and or trains:

> *But, because we are part of Intelligent Transportation System (ITS), a lot of people don't realize that our buses are computers. And if I'm a person that wants to do some harm then I'll hack into your system and see everything. So, we kind of give them that insight, because routinely, operators and staff do not get that insight in cyber. So, we let them know that this is what we do now in 2022.*

Interview Question 2, Theme 4: Verification and validation of code for data traffic. Secondly, in an open-ended response, participants felt highly about security regulation such as verification and validation of code for data traffic from end to end especially if their global software supply chain will go into consumer production, especially vehicular units, from vehicular embedded network to mobile network, P03 (Product and Program Manager for SAS Institute) increasingly believe that:

> *We do use a third-party products and code as well as internally validating and verifying that code works with our internally developed software. We also take into account regulatory and laws from the various countries that we are in. We also use other*

> *agencies or tother ISO standard for example to check that security regulations or requirements are met.*

Interview Question 2, Theme 5: Risk management and threat reduction planning to protect safety messaging systems. In an open-ended question, participants felt highly about risk reduction planning, threat reduction planning for connected systems, risk analysis and assessment to protect safety messaging, P03 (Product and Program Manager for SAS Institute) increasingly suggest the need to be constantly aware of new threats within critical software products:

> *So, it is a constant evaluation periodically over quarter to quarter of what might be changing and new developments, new viruses, bugs, anything that is out there that we need to be aware of. We take that review and take it into a complete review board. As a global company, we actually have several of those review teams that go through the code and sometime because we are a global, we have regional department that go through specific laws for the legal team, security team, and the software development team, R&D team, you name it.*

Interview Question 3, Theme 1: Vehicle security for cars, fleet buses, and or rail safety messaging system are both internal and external program requiring security assessment constantly. In an open-ended response, participants felt highly that vehicle security for cars, fleet buses, and or rail are both an internal and external program requiring internal security assessment and external security assessment every quarter, P02 (Executive Director for Safety, Security, and Quality Assurance) is compelled to do so:

> *So, the misconception is the technology is going to lead me and I don't have to use my senses and can rely on technology 100%. And what happens with that is it means when you rely on technology, and if technology does not work, you can get hurt.*

Interview Question 3, Theme 2: Misconception that vehicles are safe to drive regardless of safety messaging system. In an open-ended question, participants felt highly about the misconception that vehicles are safe to drive, P04 (Cybersecurity Manager for a top cybersecurity organization) mentions that most driver's think in-vehicular Wi-fi are safe which connects directly to safety messaging system:

> *The biggest misconception is the in-vehicular Wi-Fi. I have a vehicle, under my vehicle's Wi-Fi. So, when I first purchased the vehicle, my phone was already connected to this vehicle when I was test driving. It automatically connected to this vehicle. And one of the misconception I would say is if it was a rental vehicle, then my phone will suddenly automatically connected to its Bluetooth, Wi-Fi etc. with all my data being shared with the in-vehicular unit. That's going to be a violation to someone like myself. Why is my phone connected to this vehicle? But now, you can go to your phone and disconnect to that Bluetooth and so not a lot of people know that you can go disconnect.*

Interview Question 4, Theme 1: Providing security awareness training for the use of internal software of safety messaging system. In an open-ended response, participants felt highly about security awareness training, for the use of their internal software of safety messaging system, P02 (Executive Director for Safety, Security, and Quality Assurance) detailed to staff the need to understand the gravity of safety messaging as a communication service for critical communication between headquarters to drivers and operators:

> *We have training that took care of counter terrorism and bombs. When it was created, it was created for bus operators and maintenance, so talking the way how they will understand the safety messaging system that is into their fleet and what is announced and how to respond. When it was presented to the administration staff and my staff at PRTC, the approach was a for our operators was a little bit lengthy. We needed to tweak that to our staff to be a bit high level, because some of it is only geared to our operators that are operating the vehicle. So, we have to really understand that depending on your data and demographic and your target audience, you may have to switch how you get your messages into the system. For instance, we saw police, we give them messages every morning within the safety messaging system before they go out. Everyone has a briefing before everyone goes into the field.*

Interview Question 4, Theme 2: Challenges on continuous connection with connected services from Software as a Service (SaaS) and Mobile Backend as a Service (MBaaS) connecting with safety messaging system. In an open-ended question, the participants felt highly about the challenges on connected services from software as a service to mobile backend as a service connected to safety messaging system units, P04 (Cybersecurity Manager for a cybersecurity organization) mentions that SaaS and MBaaS companion application isn’t really all that secure:

> *Using OnStar. We've been having problems going to a remote area, an area where we need our vehicle to climb a very steep terrain, go into a remote site that isn't the big city, where there is not much signal that couldn't use any Wi-Fi. When we didn't have Wi-Fi, we also lost connection to OnStar with live navigation guidance, speed and traffic alerts, and crisis response. Because we lost signal through our phone, we also lost signal with OnStar. Though, traditionally, OnStar generally is a connected service via satellite, the signal capacity in the area was being blocked that we couldn't make connection. With that, we felt unsafe.*

Interview Question 6, Theme 1: Passive monitoring of connected systems particularly safety messaging systems. In an open-ended response, participants felt highly about passive monitoring of connected systems, particularly in safety messaging systems, P01 (Network and Security Operation Engineer for a top cybersecurity group) mentions surveillance monitoring of threat is a turnkey ingredient to curbing out threats:

> *I'm willing to do passive monitoring within exchanges in web transaction, exchanging document, data estate within mobile and connected network to escalate anynetwork abnormalities, ifnecessary.*

Interview Question 8, Theme 1: Institutionalizing a secure standard to manage risk on safety messaging system. In an open-ended response, participants felt highly about institutionalizing a secure standard to manage risk for protecting data for safety messaging system, P01 (Network and Security Operation Engineer for a top cybersecurity group) and P04

(Cybersecurity Manager for a top cybersecurity group) mentions a secure standard use, but are not particular to any organization:

> *For our automotive client, there are several key contributors to secure standards. We would end up using NIST cybersecurity framework. This allows our network organization to further manage any types of cyber risks. We also are mandated to use secure vehicle by design. This further allows our organization to systematically manage, analyze, and create a risk planning options for the enterprise. We also need to detection and response planning within any incidents involved. Lastly, we need to provide secure updates to the clients.*
>
> *One that we use is the NIST 800-53. That is more security driven, so you know right there that there is a lot of best practices related to a lot of information systems. It is more technical. There is less risk. We can compare it to ISO 27001 which has more risk. You know for our own organization. So, the NIST kind of works hand in hand for what we want to use it for. Because we want less risk and more production out of what we are doing. And so, the more technical it is, the more we are able to work and re-engineer our security measures.*

Interview Question 8, Theme 2: Using an overarching framework for institutionalizing a vehicle security improvement framework. In an open-ended question, the participants felt highly about using an overarching framework for institutionalizing a vehicle security improvement framework for safety messaging system, P04 (Cybersecurity Manager for a cybersecurity organization) and P03 (Product and Program Manager for SAS Institute) mentions:

> *There's a lot out there. There are different measures and different methods to approaching safety messaging system to protect against hackers. There's no particular framework you can use, but I personally would utilize SOC 2 security framework, as it is what some major organization really use to protect customer data. That is one of the most important aspect, the customer data. You want their data to be protected, from connecting their cellphones attached with various types of data format from pictures, text messages, email. Those types of critical asset could leak and instantaneously become a security incident and become vulnerability for auto manufacturers, as you don't want customer data to have unauthorized access.*
>
> *In the engineering side, there is the NHTSA mandate called Cybersecurity Best Practices for Modern Vehicles and also Automated Driving Systems 2.0, IPA also has created what it's called Approaches for Vehicle Information Security, ISO has ISO 26262, ISO 21434, and ISO 24089, SAE J2735, SAE J2945/1, SAE J2945/1a for connected car and minimum requirement compliance for production. For vehicle back end services, ISO 24089.*

Interview Question 8b, Theme 1: Institutionalizing a vehicle security improvement framework. In an open-ended question, the participants felt highly about going as far to institutionalizing a vehicle security improvement framework for safety messaging system, P04 (Cybersecurity Manager for a cybersecurity organization) mentions that technology changes all the time:

> *As always, we never know it all. As always, there's room for improvement and so there's always something to learn. I always am a student to security. I always want to collaborate with other teams from development to security in terms of techniques we can use on certain vehicular security improvements within SaaS and MBaaS products. Hackers you know, you have to learn how to think like them. Because the one that is trying to break into your system don't know anything much about your system. So, you'll know how to put those security measures in place. There's always something to learn. Technology changes all the time.*

Table 2 suggested the themes and codes that have occurred within the semi-structured interview. Code are the keyword or key phrases, or key text, that has been used to promote the ongoing themes from the most popular answers of each participant respondents. The themes and excerpts were represented as *variable* 1 through 15, as the reoccurring themes throughout the conversations with the skilled subject matter experts. Together with the themes are the codes frequently been learned by the qualitative analysis software to gain recognition of the popularity within the subject's sentiment. The themes are based on the participant's acknowledgement to their own knowledge, skills, and abilities within the vehicle ad hoc network industry, particularly when it pertains to the safety messaging system. A frequency distribution also suggested that a security protocols, security framework, security compliance, and framework are top overarching themes from the semi-structured conversation.

Table 2

Themes and Codes

		Frequency	
Variable	Total	Themes andor Excerpts	Code
Variable1	1	Visiting security protocols and security framework annually	Security Protocols; Security Framework
Variable2	1	Cyber projects within vehicle ad hoc networks should focus on dataprivacy	Data Privacy on Vehicle ad hoc network
Variable3	1	Distributed teams across safety messagingsystem	Distributed teams; Stakeholder collaboration
Variable4	1	Cyberattacks in safety messaging systems are both public andprivate sectorproblem	Cyberattack
Variable5	1	Automotive and public transitgroups require periodic use of vulnerability and risk assessment program	Risk Management; Vulnerability Management
Variable6	1	Verification and validation of code for datatraffic	Verification and validation of code
Variable7	1	Risk management and threat reduction planning to protect safety messaging systems	Threat Reduction Planning for connected vehicle; Risk Analysis and Assessment for connected vehicle
Variable8	1	Vehicle security for cars, fleet buses, and or rail safety messaging system are both internal and external program requiringsecurity	Internal Security Assessment; External Security Assessment

		assessment constantly	
Variable9	1	Misconception that vehicles are safe to drive regardless of safety messaging system	Vehicles are safe to drive
Variable10	1	Providing security awareness training for the use of internal software of safety messagingsystem	Security awareness training for internal programs in safety messaging system
Variable11	1	Challenges on continuous connection with connectedservices from SaaS and MBaaS connecting with safety messagingsystem	Safety Messaging Systems are network dependent
Variable12	1	Passive monitoring of connected systems particularly safety messaging systems	Passive Monitoring
Variable13	1	Institutionalizing a secure standard to manage risk on safety messaging system	Security compliance to regulation
Variable14	1	Using an overarching framework for institutionalizing a vehicle security improvement framework.	Overarching Framework
Variable15	1	Institutionalizing a vehicle security improvement framework	Institutionalizing a framework
Total	15		

**n*=15

Table 3 suggested the themes and its reoccurrence within the uploaded textual data from Atlas.ti and NVivo. From the highly ranked themes and codes from the textual data, ranked themes were presented with the highest counts among all of the suggested variable 1 through 15, ensuring that the transposed textual data are of significant relevance to the conversations. Analyzing the sentiment of each participants populated significant themes that had surfaced within the Atlas.ti and NVivo generating high likelihood of reoccurrence from various variables. The selected themes with the most frequency achieve the benefit of most visibility within the subject matter and phenomenon. Moreover, these allowed to focus on the overarching thematic framework from an organized approach.

Table 3

Top Themes and frequency

Frequency			
Theme	**Code**	***n***	**%**
Major Theme 1			
*Visiting security protocols and security framework annually	Security Framework; Security Protocols	77	20%
Major Theme 2			
*Institutionalizing a secure standard to manage risk on safety messaging system	Compliance;	98	20%
Major Theme 3			
*Using an overarching framework for institutionalizing a vehicle security	Security Framework	89	20%

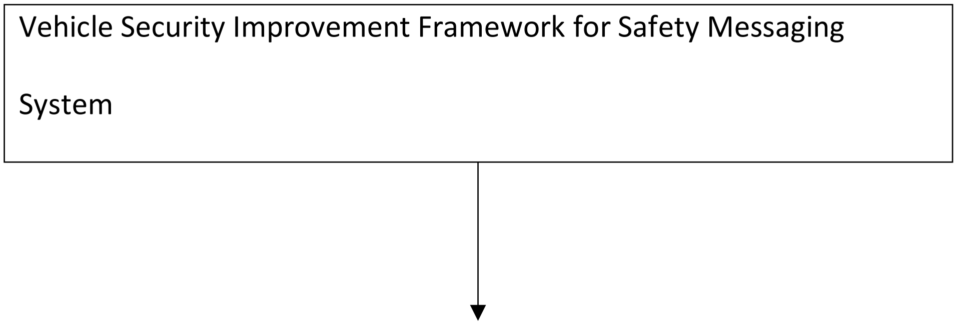
improvement framework.			
Major Theme 4			
*Automotive and public transit authority agencies require periodic use of vulnerability and risk assessment program	Vulnerability Management	64	20%
Major Theme 5			
*Institutionalizing a vehicle security improvement framework	Security Framework	72	20%
Total			100%

**n*=5

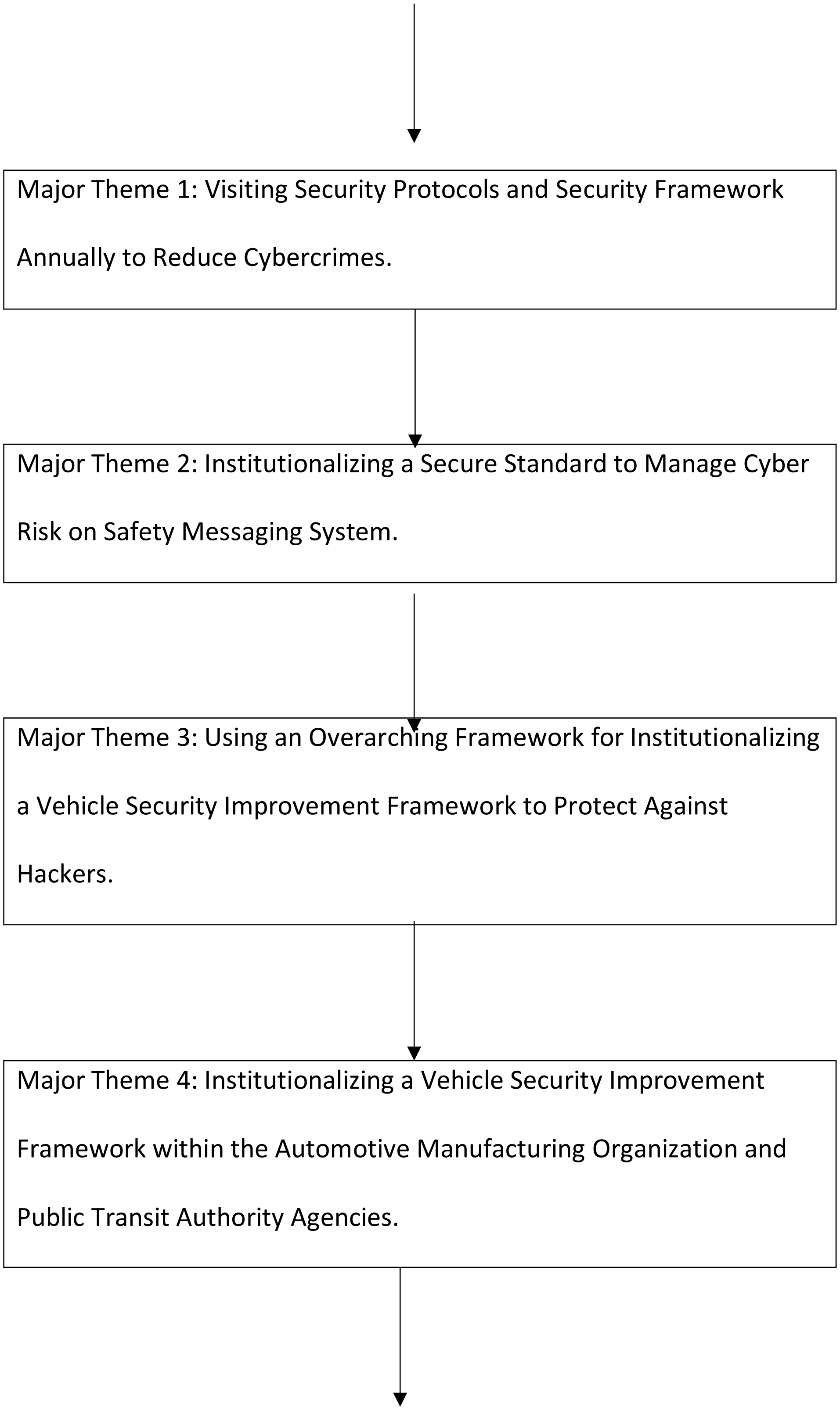
Figure 4 showed the thematic frameworks which were not an inclusive list, but an attempt to rework, reengineer, and redefine security measure for safety, protection of assets, secure data privacy on a safety messaging system component connected to any software as a service or mobile backend as a service. The thematic framework is the extracted coded excerpts from the themes and top themes converted into a detailed requirement for an automotive organization and or transit authority managing cars or fleet buses, respectively.

Figure 4

Thematic responses from open-ended questionnaire



Vehicle Security Improvement Framework for Safety Messaging System



Major Theme 1: Visiting Security Protocols and Security Framework Annually to Reduce Cybercrimes.

Major Theme 2: Institutionalizing a Secure Standard to Manage Cyber Risk on Safety Messaging System.

Major Theme 3: Using an Overarching Framework for Institutionalizing a Vehicle Security Improvement Framework to Protect Against Hackers.

Major Theme 4: Institutionalizing a Vehicle Security Improvement Framework within the Automotive Manufacturing Organization and Public Transit Authority Agencies.

Major Theme 5: Automotive and Public Transit Authority Agencies

Require Periodic Use of Vulnerability and Risk Assessment Program

The thematic responses from open-ended questionnaire was generally retrieved from the top themes and frequencies evolved through the coding procedure. The thematic responses attributes as the relative precursor scenario and its answers to the conceptual framework question seen in Chapter 1 and is a precursor to the general findings which is visited in Chapter 5. The secure standards from which most of SAE J2945/1 (March 2016) and SAE J2735 forBSM data limits data frames for which light vehicles require minimum performance requirements. This is a set of transmission criteria for which a critical communication and events communication through BSM must be secure through Over the airsecurity.

Chapter Summary

Included in within the Chapter 4 were the set of qualitative outcomes represented by the predefined subject matter experts within vehicle ad hoc networks. Interpretation to vehicle safety improvement framework (VSIF) were subjective to role and capacity within the organization. Many organizations required safety standards for data, protection of privacy, and layers of privacy before simulating an event response to connected devices within vehicular units especially as it related to the transportation sector where fleet buses, rails, and consumer vehicles are looking to engage in real time. Safety, security of connected devices, and data mining, protection of assets, seemed to be a reoccurring theme from the interviews where safety messaging systems are indicative of a 360-approach to both physical and cybersecurity.

Critical events, event response systems, and critical information were further saturated from the in- depth answers of our subject matter experts. Chapter 5 included the conclusion, summary of findings, and relationship of the selected research question to the selected problem statement.

Chapter 5: Discussion and Conclusions

The qualitative research exposed improvement framework aspects from specific problems that might arise within various vehicular ad hoc network (VANETs) technologies, in particular production vehicles that carry the safety messaging system, with its association with automotive informatics security, built through integration and execution, as they would affect many integral systems and platforms. The purpose of the proposed qualitative study is to explore the vehicle security improvements framework (VSIF) in the safety messaging system to protect against external hackers. Defining hackers within vehicle ad hoc networks mean being a *blackhat*, an adversarial attacker, and or a state sponsored attacker trying to penetrate a vehicular hardware and software products triggering innocuous effect such as subsequent indiscriminate relay to flood the broadcast dissemination of communication nodes, which may involve initiating broadcast storms within direct communication lines, or spontaneously affecting the network crafting a partitioning issue with the safety messaging system, to name a few. The overarching research question was, “What are the possible vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers?”

This vehicle security improvement framework VSIF study used an exploratory qualitative design, practically employing about 7 demographic questions, supporting to about 10 semi-structured interview questions, which also include probes that were used until data saturation were in effect. The exploratory option allowed the available 6 subject matter experts (SME) to be part of the study and become participant respondents without the need for a huge population sample. The population estimate who represented as the participant respondents came from various backgrounds from network operations, security operations, federal cybersecurity contracting, transit authority organizations that work within the automotive sector that were divided in different research subgroups. Participation merits both technical and non-technical backgrounds in their approach to securing safety messaging systems in either use of production vehicle, fleet buses, and railroadsystems.

All the semi-structured interviews were held virtual between the primary investigator and the work participants also acting as participant respondents for the exploratory study with high confidence highlighted for each participant's privacy of personal data to both audio recordings and audio transcriptions. De-identification of personally identifiable information that indicate names of specific job functions were anonymized indicating labels from P01 through P06. The use of physical storage using a local hard drive to save locally recorded conversations from Zoom, Skype and Citrix were labeled with file names P01 through P06. Data flow and data localization techniques were utilized much throughout the research project to avoid copying and storage of data from and to overseas data centers.

The use of virtual communication tools such as Zoom.com were utilized to capture various behavioral nuance, subjective nuance, and human sentiments from dedicated subject matter experts with the intent to highlight various knowledge, skills, and abilities (KSA) within the vehicle ad hoc network in particular their interaction with operating the safety messaging system. Since the subject matter experts were distributed across various geographical locations across the continental United States, the use of digital communication tools had been most imperative to initiate and inhibit a seamless interview process. During the initial phase of recruitment process, conversation with the human subjects or participant respondents at the briefing prior to the time of the interview, the participants were given the right to abandon the study, should they feel some level of discomfort before, during, or prior to the initiation of the interview.

Limitations of Study Findings

Limitations by recruitment present throughout the exploratory qualitative study. Given that the amount of time to get an approval between a Colorado Technical University Proposal Board and the Institutional Review Board committee to get to the semi-structured interview require less time for all parties to review, given such the review of the research plan require an escalated approach to reach the committee, research supervisor to communicate the requirement or change, primary investigator editing recruitment procedures and plan will be based on whether the committee accepts the research plan ahead of the schedule, or within the schedule. The recruitment timeline was not at all enough to get the subject matter experts ready for the qualitative interviews. Although some research participants had expressed that the time from the first point of contact to recruitment is rushed, some avoided the research interview invite because of the short notice, while some had agreed upon joining the research project as they want to be part and involved for something that will be beneficial within the areas of automotive informatics security, cybersecurity, and computer networks within the vehicle ad hoc network.

Limitations by sampling challenges presented throughout the exploratory qualitative study. The exploratory qualitative study focused on recruiting participant respondents (n = 06) who live in geographically dispersed areas within the continental United States who work within the areas Vehicle ad hoc network technologies. Recruitment was slow paced as many individuals are just getting back on track after multiple pandemic waves such that of the SARS-COV-2 (COVID-19) hit population centers and posted logistical challenges. During the beginning of the exploratory qualitative study, we had the first multiple waves of the pandemic, and the Colorado Technical University Proposal Board and Institutional Review Board committee all wanted to shift toward doing a virtual meeting solution for most studies. At the time of recruitment, the Colorado Technical University Proposal Board and Institutional Review Board committee had shifted guidance to allow both virtual and on-site research study collection. Requirement to do a site permission was also imperative for multiple automotive organizations, if on-site research study would be an option. Due to rushed timeline, less contingencies, and limited availability of organization's POCs to get the required participants during the rushed recruitment period, multiple organizations have declined. I have dropped the on-site option and had move toward the virtual study collection to qualify at least ten candidates through various social media channels such as LinkedIn, journal members of ResearchGate, Intelligence Vehicle Network forums, and journal members of ORCID within the field of Internet ofVehicles. Since it was a qualitative study, there required less focus on high sampling ratio, but focused more on the sampling quality, as being the only requirement as coming as a subject matter expert with knowledge, skills, and abilities within the vehicle ad hoc network, as theywere mostly unique within field. Ten human subjects or participant respondents were planned and had been uniquely recruited and have been available within various social media channels. However, the success of the sampling method was heavily dependent on the ability to contact most potential participants.

Limitations to transferability challenges presented throughout the exploratory qualitative study. As the results of the study were very specific to the small population size or unique environment being within the vehicle ad hoc network areas. It was far too difficult to transfer the set of findings toward other population groups. As many other researchers may use a different sampling method and techniques, sampling size, or sampling group, it would yield a very unique set of findings that come from various behavioral and sentiment analysis prior to gaining a thematic framework design. Because of such uniqueness, transferability could be non-linear option by nature and non-applicable or applicable based on the obtained context of the succeeding research group, individual primary investigator, and research committee. The generalizability would only be an option unique toward quantitative methods, however while the transferability may or may not be an option based on how selective claims patterned the original findings. Transferability could be an option if multiple organizations were participating, volume of individuals doing field work have multiple findings that have similarity, length of collection session were in the same timeline, and the period of time by which a data was collected would have presented a unique set of finding that have truly a parallel set of data points from previous research.

Limitations to data trustworthiness challenges presented throughout the exploratory qualitative study. Since the original study methodology leaned toward exploratory qualitative study, there required less stress about validity and reliability, which were concepts consumed most throughout quantitative method concept. The exploratory study had to use a triangulation to establish credibility, transferability, confirmability, and dependability. These were inherent functional requirement required to pursue a valid qualitative research. Withsuch goals, there was less use of instruments to establish metrics, as would a quantitative method would actually use. With credibility, findings were unique set of data established within the semi-structured interview allowing for confidence that the subject matter experts used specific methodical framework within their response within the research questions. Meanwhile, the confirmability was when the set of findings were looked as a neutral statement that could be utilized to look if participant respondents do not possess any potential bias and personal motivation within the type of research. Additionally, the dependability was a concept utilized if study findings used by other researchers pursuing the same research would have a consistent output. Generally, these triangulation techniques were not always in sync, and not too many researchers would generate a similarfinding.

Interpretation of Study Findings

The interview required briefing of the subject matter experts before the actual semi-structured interview. Likewise, the interview also required the subject matter experts to be debriefed thereafter the responses were taken. The subject matter experts or the research participants were told of the interpretation procedures of the study findings, after the results were concluded.

Following up with the statement from each of the participant respondents, the subject matter experts were scheduled within several interview blocks to initiate the process of the data collection process continuing in a semi-structured interview. The respondents were hand selected from the area of vehicle ad hoc networks. The qualified participant respondents remained calm and supportive of the study. As the questionnaires were being answered one by one, respondents come from various backgrounds, from analyst roles, mid-level program managers, to mid-level c-suite roles that all interact within the field of Internet of Vehicles.

Following up with the interpretation of the study findings, the interpretation waslimited to the use to thematic analysis software which involved the use of multiple qualitative analysis software as a service platform from NVivo and ATLAS.ti. The interpretation also included several coded words extracted from excerpts that were purely subjective to the programmed variable word across the software. With it, machine learning and sentiment analytical key phrases came out as themedmessages.

Following up with the interview questions, probes were utilized to further extract the individual narratives and inferences from each of the participant respondents, until such data saturation occurs within the answers. These inferences are either practice related or industry specific guidance which most of the participant respondents have related too. Many of the participant respondents have completely answered all 10 interview questions. Meanwhile, several of the participant respondents have skipped answering multiple questions as it does not directly relate to their technical workload.

Following up with the data collection, the recordings were set to local recording for Zoom, Skype, and Citrix. Most of the local audio data have to be preserved as an encrypted-at-rest file on the primary investigator's Apple MacBook computer, and a physical backup storage from an Apple iMac computer. The access to the encrypted-at-rest file is protected with an identity management technology and access control as a service feature such as biometric authenticator from the primary investigator's Apple MacBook computer. The local audio data can only be access solely by the primary investigator. Interviews were conducted virtually to about 55-minute time frame.

Following up with the analysis, axial and open coding were utilized in most sections of the analysis whereby it defined several key aspects and areas of texts, key terminologies, phrases and sub-phrases, descriptors, and identifier mostly from the passage inserted. The use of NVivo and Atlas.ti qualitative analysis software allowed for transposition of the verbal transcription of the key responses from the subject matter experts and subsequently allow the management of coding procedure. The transposed text required the use of individual coding assignment to each of the verbal transcription. The coded verbal transcription exposed many categories that procured major and minor themes within each question. The themes were categorized and placed in the order of priority as top themes used within the thematic framework. The major themes are predominantly succinct within the topic Exploring Vehicle

Security Improvement Framework in Safety Messaging System to Protect Against Hackers. These major themes were brought down and condense to the top five emerging themes:

Major Theme 1: Visiting Security Protocols and Security Framework Annually to Reduce Cybercrimes

The major theme indicated that the majority of the participants have high likelihood to visit security protocols and security framework annually to protect data assets from becoming a variable to a progressive attack or threat landscape especially as it relates to hardware and software configurations of the safety messaging systems. Five out of six subject matter expert participants agreed with the realization of an annual security framework and security protocol visitation would be more economical versus mitigating an impending attack. The major sentiment was that the management and executive level management should control functionality to deliberately: provide messaging to all risk and vulnerable physical areas for the drivers, guidance from top-to-bottom to initiate security framework practice, controls, and management toward delivery of security assessment exercises, and providing feedback control technology for drivers to initiate driver assisted updates for vehicle-to-vehicle communication.

Major Theme 2: Institutionalizing a Secure Standard to Manage Cyber Risk on Safety Messaging System.

Major theme indicated that having a secure standard to manage risk on safety messaging system is a requirement to most automotive organizations, vendors, and client groups pertaining to critical assets such as safety messaging systems that affect safety of drivers, motorists, and bystanders. Security could be both in the paradigm of physical and digital in nature. Maintaining security within in vehicular software units particularly that enables safety messaging system had been disparate in most cases from manufacturer to manufacturer and vendor, in so the use of many security standards and framework are utilized which make the matter much worse. Four out of six subject matter experts agreed that institutionalizing a secure standard would be much practical to manage risk on safety messaging system and become cornerstone of change management and technology redevelopment in ensuring security hardened products are deployed throughout the production and post-production environment. The participants agree with the lack of secure standards and utilization of many compliances that qualifies as a complex procedure.

Organizations vary by strength, especially risk appetite, in so the utilization of a secure standard especially like from the NIST or SOC2 could be a matter of a streamlined decision from the stakeholder management.

Major Theme 3: Using an Overarching Framework for Institutionalizing a Vehicle Security Improvement Framework to Protect Against Hackers.

Major theme indicated that majority of respondents agree with the need for an overarching active framework such that of a vehicle security improvement framework (VSIF) for most automotive manufacturing providers and transit authority client groups as there are multiple cybersecurity framework currently being used within modern vehicles today. Five out of six participants agreed that overutilization of risk and compliance framework within several areas comes with a price that the use of multiple frameworks would allow for crossovers in multiple regulatory frameworks. As there are many security frameworks for VANETs, SOC 2 would be a good choice for any organization that capitalized on customer data protection. Meanwhile, there is the NHTSA mandate called *Cybersecurity Best Practices for Modern Vehicles* and also *Automated Driving Systems 2.0* that can also be utilized by automakerand transit executive as they deploy autonomous technologies. Additionally, the IPA alsohas

created what it's called *Approaches for Vehicle Information Security* as these can be utilized by many automakers and transit executives to deploy hardened software for the future. Lastly, International Standard Organization (ISO) has predefined ISO 26262, ISO 21434, and ISO24089 for connected car and OEM (hardware + software) production security as these overlooked at OEM devices carefully from deployment, production, to post-productionmethodologies.

Major Theme 4: Institutionalizing a Vehicle Security Improvement Framework within the Automotive Manufacturing Organization and Public Transit Authority Agencies.

Major theme indicated that the most participant respondents agreed that institutionalizing a vehicle security improvement framework were imperative to a successful transportation organization whether technology groups helping secure hardware and software products within automotive manufacturing client groups or transit authorities. Five out of six participant respondents agreed that the need to collaborate with other teams from development to security in terms of techniques can be a strategic advantage while improving the level of uncertainty of an software hardening towards safety messaging systems, while initiation of a continuous vehicular security improvements could come as a refreshing standard within Software as a Service (SaaS) and Mobile Backend as a Service (MBaaS) deployed products, specific to vendors, which could strengthen the production integrity of critical assets such as safety messaging system.

Major Theme 5: Automotive and Public Transit Authority Agencies Require Periodic Use of Vulnerability and Risk Assessment Program

Major theme indicated that most participant respondents agreed that automotive manufacturing organization and public transit authority must have adequate vulnerability management and risk assessment programs within their premises. The protection from structural layers were inhibited by top leaders within the automakers and transit authorities and amended when it is necessary and required to strengthen operability of most connected software products particularly safety messaging systems. For most automotive organizations and transit authorities, the attack landscape for moving vehicles and fleet buses have never before become more critical today as the ability to potentially override a vehicular device and access critical vehicular components that could potentially paralyze access from the driver and motorist alike, assuring accident could be as imminent as planned by an attacker. Executive leaderships understood that as the attack landscape become far more spread out than just a safety messaging system, controlling specific access to technologies would become more crucial, and surveillance technologies would be involved as desired by automakers and vendors. The reality of periodic vulnerability and risk assessment programs have to be utilized to protect and save lives as much so at the state level, and the community level, to prevent the likelihood of any chances of cyber interference.

Practice Implications of Study Findings

This study extracted three major points from the findings. Consider these action plan suggestions when building an effective vehicle security improvements framework: (a) automotive organizations and transit authority leaders have to manage vehicle cyber risks throughout the vehicle lifecycle, (b) automotive organizations and transit authority should be involved in engineering a secure vehicle by design, and (c) engineering vendor teams should detect and respond to major incidents within the vehicle lifecycle. The Practice Implications of Study Findings are generally the thematized responses taken from the original research questions within Chapter 1, provided by the subject matter experts as responses within Chapter 4 and extracted as themes, while fully discussed within the background of study within the Chapter 2 Review of the Literature discussed by majority of the topics that contributed to the research question.

The potential to massively harbor critical data within a vehicle is an imminent matter for most automotive organization, much so the safety aspect that could potentially be at risk when it comes to digital access to vehicular devices that could override a vehicle in operation. The automotive organizations, vendors, and client groups should join forces in managing potential threats throughout the lifecycle of vehicle and fleet as any major disruption could potentially affect lives and harm motorists. The engineering environment should carefully curate secure vehicles throughout the research and development phase of a potential production vehicle, as there may be curative aspects that could be organized to ensure safety and security of connected products such that of safety messaging system. Nevertheless, automotive organizations and transit authority providers should be able to contribute to managing secure vehicles in post-production.

Major Finding 1: Automotive Organizations and Transit Authority Leaders have to Manage Vehicle Cyber Risks throughout the Vehicle Lifecycle. From Cyber Risk Officers, Cybersecurity Managers, and Cybersecurity Analyst within the automotive organization and transit authority partners all does require to utilize a vehicle safety improvement framework and thoughtful leaders have to mobilize and manage vehicle cyber risks throughout the vehicle lifecycle. The general findings have found that too many automotive organizations and transit authority agencies required proper take on compliance planning and management to better manage vehicle cyber risks throughout the vehicle lifecycles, a regulatory frameworks could be held to different set of standards, thus increasingly diversified requirements for various agencies, and automotive manufacturing organizations.

Major Finding 2: Automotive Organizations and Transit Authority Should Be Involved in Engineering a Secure Vehicle by Design. Subject matter experts have agreed that automotive organizations and transit authority groups and vendors should be included in the future engineering works from pre-production and post-production meetings when creating a secure vehicle by design as secure vehicles can encompass areas within development, production, and post-production. When it came to planned a connected system, particularly that of safety messaging system, automotive organizations and transit authority partners should be priority stakeholders in acknowledging practical implications of poorly designed and highly designed security environment withinvehicles.

Secondly, the subject matter experts agreed that an overarching framework could possibly become a suitable standard for more automotive organization looking to enforce safety within the digital car ecosystem. A McKinsey & Co. finding have also found that there were five systemic areas of vulnerabilities which are the following: a) in vehicle services, b) OEM back-end service, c) infrastructure and third party, d) enterprise technology, and e) production and maintenance.

Major Finding 3: Engineering Vendor Teams Should Detect and Respond to Major Incidents within the Vehicle Lifecycle. Upon further investigation, engineering vendors and transit security contractors should be allowed to respond to major incident within the vehicle lifecycle. Whereupon, the engineering vendors take crucial attention to the safety messaging system or basic messaging system (BMS). The software area was part of Infrastructure/third-party services that highlighted security issues upon discovery techniques and indicative of vulnerability within car-sharing application, as well. Also, these third-party services had general exposure to personal data, backed by our subject matter experts. With production vehicles and transit trains and fleet adjoining the problem, in-vehicle services were also seen as one of the most vulnerable areas, with the vulnerabilities specific to infotainment system, thus gaining control to multitude of functionalities within microphones, speakers, and navigation. A periodic use of risk and vulnerability management planning to increase safety scores of their fleets and production vehicles can be necessary.

Researcher Reflections

I learned that there were many variables to conducting an exploratory qualitative study. Firstly, gathering facts for the literature review allowed me to craft a narrative and see how other security researchers have personally researched and seen high risk threat, exposures, and vulnerabilities within a connected system environment particularly within in-vehicular units such as safety messaging systems. As my general interest spiked further, realizing how safety and security are closely aligned and tightly related, especially as it relate to automotive informatics security, have further redeveloped my conceptual framework to aligned with the perspective of my research question: what are the possible vehicle security improvements framework in the safety messaging system to protect against external hacker? Furthermore, realizing the research questions would validate certain aspects of the literature review given the tremendous assurance from the cybersecurity researchers gathering unique set of qualitative and quantitative data previously validated and doing my own semi-structured interviews with the subject matter experts also put perspective into how the in-vehicle service, OEM back-end service, infrastructure and third party service, and enterprise technology service all serve as layers of connectedness within the vehicles cybersecurityecosystem.

Secondly, understanding that these components could further expose major gaps within critical asset such as general exposure of the safety messaging system could further paralyze automotive sector's attempt for higher safety ratings and major transit authority's unique presence within the market as a market leader in some regions. There require further study within in-vehicle service security solutions, OEM back-end service security solutions, infrastructure and third-party service security solutions, and enterprise technology service security solutions, should any researcher come up to strengthen the divide of the vehicle's ecosystem. It is definite that my understanding within the automotive informatics security field has further evolved. Also, my elaborate understanding of the vehicle security lifecycle increased within the allowance of such exploratory research study. Being able to analyzed the sentiments of my subject matter experts, incorporated them as a theme, created a vehicle security improvement framework charter, and assessment further strengthened the claim that the safety messaging system lack the unique security feature that were required to ensure safety and security is provided by design.

Recommendations for Further Research

The qualitative study was designed to explore the vehicle security improvement framework in the safety messaging system to protect against hackers. The limitation of a connected mobility particularly when vehicles, fleet buses, and or trains that are in transit as it relates to one connected platform can sometimes be disparate, and sharing data to improve overall efficiency, user experience, and safety and security for the driving user may require aset of an overarching set of vehicle security improvement framework as connectedness to critical systems such as safety messaging system is imperative at all cost from the production environment for vehicles, fleet buses, and trains that tend to be more exposed to the daily traps of the real-world cybercrimes. With such expansive qualitative data provided by the automotive industry, its network and security vendors, the industry is looking at a loophole of issues that are continually becoming a trend as vehicular environment become more digital, aggressively vulnerable, and massively scaled. Based on the findings and limitations withinthe study, the following topic must further be developed for future research: a) in-vehicle service security, b) OEM back-end service security, c) infrastructure and third-party service security, and d) enterprise technology service security.

Recommendation 1. Recommendation 1 is the *in-vehicle service security solutions* that are required for various car mobility networks to be protected. Further research on this units can expose local access to infotainment systems, telematics and CAN bus units that are tremendously vulnerable within a connected vehicle, fleet buses and trains. These leaves the connection toward critical systems further unsafe such safety messaging system and left at higher risk exposure. Exploration and analysis of further study within in-vehicle service security solutions as it relates to vehicle security improvement framework should be further granted more research study, funding, and efforts.

Recommendation 2. Recommendation 2 is the *OEM back-end service security solutions* that are required to treat malware infection from the backend units making connected laptop units from fleet buses and trains exposed, or could be unusable if left untreated generally affecting personal data and leaving critical systems such as safety messaging system left exposed. Vehicle data exposure could leave personally identifiable information and digital registration information of drivers and operators for both from personal vehicles, fleet buses, and trains exposed for denial of service attacks. Exploration and analysis of further study within OEM back-end service security solutions as it relates to vehicle security improvement framework should be further granted more research study, funding, and efforts.

Recommendation 3. Recommendation 3 is the *Infrastructure and third-party service security solutions* that could be utilized to prevent at home and at-facility EV chargers controlled by accessed Wi-Fi technologies. Also, prevention of further security issues within connected car-sharing application that could employ a stricter guidance in connecting to critical systems such as safety messaging system. Exploration and analysis of further study within the Infrastructure and third-party service security solutions as it relates to vehicle security improvement framework should be further granted more research study, funding, and efforts.

Recommendation 4. Recommendation 4 is the *Enterprise technology service security solutions* that may further be utilized to prevent any memory vulnerability at most cloud providers exposed. These exposures could be leak data including passwords, API keys, and tokens from network restricted access. A major attack could mean that the OEM's automotive cloud could also be left exposed via access to third-party service solutions and tier-1 supplier network. Exploration and analysis of further study within the enterprise technology service security solutions as it relates to vehicle security improvement framework should be further granted more research study, funding, and efforts.

Conclusion

The purpose of the qualitative study is to explore the vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers. The research participant consisted of 6 subject matter experts as participant respondents who expressed interest and came willingly at the study. The participant respondent's backgrounds came from wide array of sectors of STEM from network operations, cybersecurity operations management, federal cybersecurity contracting, transit authority organizations that work within the automotive sector, who was available at the time of the research.

This research question of the study sought to build improvements to answer to the following research questions:

Q1: What are the possible vehicle security improvement framework (VSIF) in the safety messaging system to protect against external hackers?

The selected type of *exploratory research* within the study will be used by the primary investigator in accordance to the conceptual design of De Langhe and Schliesser's of explorative research to make room for incremental improvement for more exploitative technologies safety messaging system for automotive vehicles. With this effort, vehicle security improvement framework (VSIF) as the improvement feature, and the safety messaging system or basic messaging system (BSM) as the exploitative technology that can be set to improve the security posture of the vehicular ad hoc networks (VANETS) which then will be harvested from the semi-structured interview that will take place with our selected stakeholders, to truly make the research method and philosophy appropriate for the research study.

The interpretation of study findings estimated and produced five major themes within the exploratory qualitative research. The study has garnered sentiments from 10 semi-structured interviews together with at least 7 additional probes during the data collection process. The 6 subject matter expert responses have to be converted to word transcription which have been saved and configured to include P01 to P06 document names for anonymity. The use of a qualitative analysis software such as NVivo and Atlas.ti had to be collect certain word transcription to perform specific axial coding to provide at least ten themes from the subject to answer the research question. The detailed five major themes are the following: a) Major Theme 1: Visiting Security Protocols and Security Framework Annually to Reduce Cybercrimes, b) Major Theme 2: Institutionalizing a Secure Standard to Manage Cyber Risk on Safety Messaging System, c) Major Theme 3: Using an Overarching Framework for Institutionalizing a Vehicle Security Improvement Framework to Protect Against Hackers, d) Major Theme 4: Institutionalizing a Vehicle Security Improvement Framework within the Automotive Manufacturing Organization and Public Transit Authority Agencies, and e) Major Theme 5: Automotive and Public Transit Authority Agencies Require Periodic Use of Vulnerability and Risk Assessment Program.

The practice implications of study findings estimated and produced three major findings within the exploratory qualitative research. The detailed three major findings were reduced from the five major themes from the study. The three main points or major findings are the following: a) Major Finding 1: Automotive Organizations and Transit Authority Leaders have to Manage Vehicle Cyber Risks throughout the Vehicle Lifecycle, b) Major Finding 2: Automotive Organizations and Transit Authority Should Be Involved in Engineering a Secure Vehicle by Design, and c) Major Finding 3: Engineering Vendor Teams Should Detect and Respond to Major Incidents within the Vehicle Lifecycle.

The applicability of the study findings to study should be continued by comparing the primary investigator's findings along with new set of compliance, security regulation, and industry standards along with the current guidance among cybersecurity framework and compliance management implementations. The addition of thematic framework to be finetuned with many subject matter experts to reduce cyber interference or breaches within connected networks on vehicle units such as safety messaging systems are increasingly important.

The recommendation for future research of study is designed to explore the vehicle security improvement framework in the safety messaging system to protect against hackers. For future reference, there have been four levels of recommendations for future research to further explore by future researchers. The recommendation are the following: a) Recommendation 1 is the *in-vehicle service security solutions* that are required for various car mobility networks to be protected, b) Recommendation 2 is the *OEM back-end service security solutions* that are required to treat malware infection from the backend units making connected laptop units from fleet buses and trains exposed, or could be unusable if left untreated generally affecting personal data and leaving critical systems such as safety messaging system left exposed, c) Recommendation 3 is the *Infrastructure and third-party service security solutions* that could be utilized to prevent at home and at-facility EV chargers controlled by accessed Wi-Fi technologies, and d) Recommendation 4 is the *Enterprise technology service security solutions* that may further be utilized to prevent any memory vulnerability at most cloud providers exposed.

For many years, the demand for connected networks in personal vehicles and fleet have left a major sinkhole in the automotive and transit service industry, its cyber defenses. The lack of major investment within cyber has left major concerns for connected networks and itsability to safely secure critical assets such as data in transit and data at rest traffic within safety messaging systems. Inclusively, major exposures left vehicular units generally exposed to further hardware damage during a cyber interference or cyberattack. Our esteemed subject matter experts all have been either involved within network operation, security operation, cybersecurity management, and transit authority clearly has stated how exposed critical assets were as hackers are extremely capable of paralyzing a safety messaging system unit.

References

Ahmed-Zaid, F. (2019, Aug 19). SAE Standard Overview of Basic Safety Message (BSM). *Ford Motors Press*.

Alkadi, O.S., Moustafa, N., Turnbull, B., and Choo, K.R. (2020). An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems. *IEEE Transactions on Information Forensics and Security*, 1164-1174. https://doi.org/10.1109/TIFS.2019.2936975.

Amel, M. M., & Guizani, M. (2019). SE-AOMDV: Secure and efficient AOMDV routing protocol for vehicular communications. *International Journal of Information Security. 18*(5), 665-676. https://doi.org/10.1007/s10207-019-00436-z.

Amin, M., & Tariq, Z. (2015). Securing the car: How intrusive manufacturer-supplier approaches can reduce cybersecurity vulnerabilities. *Technology Innovation Management Review, 5*(1), 21-25. https://doi.org/10.22215/TIMREVIEW/863.

Aneetha, A. S., & Sundan, B. (2015). A dynamic intrusion detection system based on multivariate hotelling's T2 statistics approach for network environments. *The Scientific World Journal.* https://doi.org/10.1155/2015/850153.

Armstrong, M., Jones, K., Namin, A., and Newton, D. (2020, Nov 13). Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Transactions on Computing Education*, *20*(4), 1-25. https://doi.org/10.1145/3421254.

Auerbach, C.F., and Silverstein, L.B. (2003). Qualitative Data: An Introduction to Coding and Analysis. *New York University Press,* 44.

Bazeley, P. (2007). Qualitative Data Analysis with NVivo. Sage Publications Limited.

Bhoi, S.K., and Khilar, P.M. (2012). SST: A secure fault-tolerant Smart Transportation system for Vehicular Ad hoc Network. *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 545-550. https://doi.org/10.1109/PDGC.2012.6449879.

Bochem, A., and Leiding, B. (2021). Rechained: Sybil-resistant distributed identities for the internet of things and mobile ad hoc networks. *Sensors*, *21*(9), 3257. https://doi.org/10.3390/s21093257.

Bouali, T., Senouci, S., and Sedjelmaci, H. (2016, Jul 10). A distributed detection and prevention scheme for malicious nodes in vehicular networks. *International Journal of Communication Systems, 29*(10), 1683-1704. https://doi.org/10.1002/dac.3106.

Boukerche, A., and Zhang, Q. (2019, May). Countermeasures Against Worm Spreading: A New Challenge for Vehicular Networks. *ACM Computing Surveys*, *52*(2), Article 34, 25 pages. https://doi.org/10.1145/3284748.

Boyatzis, R.E. (1998). Transforming qualitative information: Thematic analysis andcode development. *Sage Publications,Inc*.

Brooks, R., Deng, J. (2012). Handbook on Securing Cyber Physical Critical Infrastructure. *ScienceDirect*. https://doi.org/10.1016/C2011-0-04434-4.

Butler, B. (2016). BMW's vision for a world of connected cars. *Network World (Online).* https://proquest.com/central/docview/1790516641?accountid=45927.

Carlier, M. (2021, Aug). Number of employees in U.S. automotive industry by sector 2010-2021. https://www.statista.com/statistics/276474/automotive-industry-employees-in-the-united-states-by-sector/

Casal, C.R. (2005). Privacy within in-car systems. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 7*(1), 66-75. https://doi.org/10.1108/14636690510578289.

Chattopadhyay, A., Lam, K.Y., and Tavva, Y. (2020, Jun 30). Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2020.3000797.

Claburn, T. (2011). Your car's next enemy: Malware. *InformationWeek – Online.* https://proquest.com/docview/888082817.

Chung, B., Kim, J., and Jeon, Y. (2016, Oct 19). On-demand security configuration for IoT devices. *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, 1082-1084. https://doi.org/10.1109/ICTC.2016.7763373.

Cord, A. and Gimonet, N. (2014, Mar). Detecting Unfocused Raindrops: In-Vehicle Multipurpose Cameras. *IEEE Robotics & Automation Magazine*, *21*(1), 49-56. https://doi.org/10.1109/MRA.2013.2287451.

Costigan, S. S., and Lindstrom, G. (2016). Policy and the internet of things. *Connections: The Quarterly Journal, 15*(2), 9-18.https://doi.org/10.11610/Connections.15.2.01.

Coventry.(2015).Globalencryptionsoftwaremarketisexpectedtoreach$2.16billionby2020; finds new report. *M2 Presswire*.https://proquest.com/docview/1650831044.

Cronin, S., and Butka, B. (2018). Self-Optimizing Image Processing Algorithm for Safety Critical Systems. *SoutheastCon 2018*, 1-5. https://doi.org/10.1109/SECON.2018.8479179.

Daneshmandpour, N., Danyali, H., and Helfroush, M.S. (2019, Nov). Image tamper detection and multi-scale self-recovery using reference embedding with multi-rate data protection. *China Communications*, *16*(11), 154-166. https://doi.org/10.23919/JCC.2019.11.013.

Davis, P. (2005). Cyber security and implications for national infrastructure. *The IEEE Seminar on Security of Distributed Control Systems,* 1-12. https://doi.org/10.1049/ic:20050251.

De Langhe, R., and Schliesser, E. (2017). Evaluating Philosophy as Exploratory Research. *Metaphilosophy*, *48*(3), 227-224. https://doi.org/10.1111/meta.12244.

Deming, W.E. (1994), "The need for change", The Journal for Quality and Participation, *17*(7), 30-2.

Deng, S., Gao, X., Lu, Z., and Gao, X. (2018, Mar). Packet Injection Attack and Its Defense in Software-Defined Networks. *IEEE Transactions on Information Forensics and Security*, *13*(3), 695-705. https://doi.org/10.1109/TIFS.2017.2765506.

De Paula Veronese, L., Auat-Cheein, F., Mutz, F., Oliveira-Santos, T., Guivant, J.E., de Aguiar, E., Badue, C., De Souza, A.F. (2021, Mar). Evaluating the Limits of a LiDAR for an Autonomous Driving Localization. *IEEE Transactions on Intelligent Transportation System*, *22*(3), 1449-1458. https://doi.org/10.1109/TITS.2020.2971054.

Durech, J., Franekova, M., Holecko, P., & Bubenikova, E. (2016). Modelling of security principles within car-to-car communications in modern cooperative intelligent transportation systems. *Advances in Electrical and Electronic Engineering, 14*(1), 49-58.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness.*SAGE Open*.https://doi.org/10.1177/2158244014522633.

Enis, M. (2015, May 1). NetObjex enters beacon market: SmartLibrary facilitates administration, messaging. *Library Journal, 140*(8). https://link.gale.com/apps/docA411752073/BIC?u=tec_online&sid=summon&xid=37a2f0f6

Evans, J. and Lindsay, W.M. (2001), The Management and Control of Quality. South-Western, Cincinnati, OH, 60-190.

Eziama, E., Awin, F., Ahmed, S., Santos-Jaimes, L., Pelumi, A., and Corral-De-Witt, D. (2020). Detection and identification of malicious cyber-attacks in connected and automated vehicles' real-time sensors. *Applied Sciences*, *10*(21), 7833. https://doi.org/10.3390/app10217833.

Federal Communications Commission. Dedicated Short Range Communication Service. *Bureau of Wireless Telecommunications*. https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service

Knowles-Flanagan, S., Tang, Z., He, J., Yussoff, I. (2021, Mar). Investigating and modeling of cooperative vehicle-to-vehicle safety stopping distance. *Future Internet, 13*(3), 68. https://doi.org/10.3390/fi13030068.

Galeta, A. and Cross, W. (2013, Jun 17). Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication. 76. https://doi.org/10.18574/nyu/9780814732939.001.0001.

Ghafoor, K.Z., Kong, L., Zeadally, S., Sadiq, A.S., Epiphaniou, G., Hammoudeh, M., Bashir, A.K., and Mumtaz, S. (2020, Sep). Millimeter-Wave Communication for Internet of Vehicles: Status, Challenges, and Perspectives. *IEEE Internet of Things Journal*, *7*(9), 8525-8546. https://doi.org/10.1109/JIOT.2020.2992449.

Giles, K., and Hartmann, K. (2019). Silent Battle” Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1-13. https://doi.org/10.23919/CYCON.2019.8756713.

Guo, C., and Bei, G. (2021). Efficient scalar multiplication of ECC using SMBR and fast septuple formula for IoT. *EURASIP Journal of Wireless Communications and Networking*. https://doi.org/10.1186/s13638-021-01967-7.

Gyawali, S., Qian, Y., and Hu, R.Q. (2020, Aug). Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8871-8885. https://doi.org/10.1109/TVT.2020.2996620.

Haber, M.J., Rolls, D., Smith, D.A. (2020). Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. *APress*. https://doi.org/10.1007/978-1-4842-5165-2_10.

Haider, S. (2020, Jul 1). A Novel Cross-Layer V2V Architecture for Direction-Aware Cooperative Collision Avoidance. *Electronics (Basel)*, *9*(1112), 1112, https://doi.org/10.3390/electronics9071112.

Hall, R. (2013). A Geoacst Based File Transfer Protocol. *MILCOM 2013 – 2013 Military Communications Conference,* 150-156. https://doi.org/10.1109/MILCOM.2013.35.

Hathal, W., Cruickshank, Z., and Maple, C. (2020). Certificateless and Lightweight Authentication Scheme for Vehicular Communication Networks. IEEE Transactions on Vehicular Technology, *69*(12), 16110-16125. https://doi.org/10.1109/TVT.2020.3042431.

Hunt, T. (2016). Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs. https://www.troyhunt.com/2016/02/ controlling-vehicle-features-of-nlssan.html.

Ibiricu, B., van der Mad, M. (2020). Ethics by design: a code of ethics for the digital age, *Records Management Journal*, *30*(3). https://doi.org/10.1108/RMJ-08-2019-0044.

Ibrahem, K. D., Rashid, A. N., & Mubark, F. S. (2021). A new deployment schema using dynamic relay vehicle to improve VANETs connectivity in urban environment. *IOP Conference Series Materials Science and Engineering, 1076*(1). https://doi.org/10.1088/1757-899X/1076/1/012035.

Ioana, A., & Korodi, A. (2020). OPC UA publish-subscribe and VSOME/IP notify-subscribe based gateway application in the context of car to infrastructure communication. *Sensors, 20*(16), 4624. https://doi.org/10.3390/s20164624.

Jackson, D. (2020). Connected cars facing a data logjam. *Urgent Communications*. https://www.proquest.com/docview/2414434297.

Kang, J.M., Tae, S.Y, Kim, E., and Jin, B.P. (2020). Lane-level map-matching method for vehicle localization using GPS and camera on a high-definition map. *Sensors, 20*(8), 2166. https://doi.org/10.3390/s20082166.

Kang, M., & Kang, J. (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PLoS One, 11*(6). https://doi.org/10.1371/journal.pone.0155781.

Kang, S., Veeravalli, B., Aung, K. M., and Jin, C. (2014). An efficient scheme to ensure data availability for a cloud service provider. *2014 IEEE International Conference on Big Data (Big Data)*, Washington, DC, 15-20. https://doi.org/10.1109/BigData.2014.7004378.

Karamete, B.K. (2021, Feb 02). An Adaptive Markov Chain Algorithm Applied Over Map-Matching of Vehicle Trip GPS Data. *Geo-Spatial Information Science.* https://doi.org/10.1080/10095020.2020.1866956.

Katkar, A., Shukla, S., Shaikh, D., and Dange, P. (2021). Malware Intrusion Detection for System Security. *2021 International Conference on Communication information and Computing Technology (ICCICT)*, 1-5. https://doi.org/ 10.1109/ICCICT50803.2021.9510161.

Keanneally, E., and Bailey, M. (2014). Cyber-Security Research Ethics Dialogue and Strategy Workshop. *2014 IEEE Security and Privacy Workshop*, *44*(2), 76-79. https://www.mdbailey.ece.illinois.edu/publications/ccr-2014.pdf.

Khan, S.M., and Chowdhury, M. (2021) Situation-Aware Left-Turning Connected and Automated Vehicle Operation at Signalized Intersections. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3064041.

Khayati, Y., & Mazri, T. (2020). Security Study of Routing Attacks In-Vehicular Ad Hoc Networks (vanets). *Copernicus GmbH.* https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-267-2020.

Kim, J., Lee, J., and Pack, S. (2019) Poster: A Vehicular Participant Recruiting Strategy for Improving Sensing Quality in Vehicular Crowdsensing. *2019 IEEE Vehicular Networking Conference (VNC)*, Los Angeles, CA, USA, 1-2. https://doi.org/10.1109/VNC48660.2019.9062811.

Kiss, G. (2019, Sep 19). External manipulation recognition module in self driving vehicles. *2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY)*, 000231-000234. https://doi.org/10.1109/SISY47553.2019.9111547.

Kolte, S.R., & Madnkar, M.S. (2014) A Design Approach of Congestion Control for Safety Critical Message Transmission in VANET. *2014 Fourth International Conference on Communication Systems and Network Technologies*, 298-301. https://doi.org/10.1109/CSNT.2014.65.

Koops, B., Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology, 28*(2), 159-171. https://doi.org/10.1080/13600869.2013.80159.

Krall, A. L., Kuhl, M. E., Moskal, S. F., and Yang, S. J. (2016). Assessing the likelihood of cyber network infiltration using rare-event simulation. *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, Athens, 1-7. https://doi.org/10.1109/SSCI.2016.7849913.

Langham, E., Thorne, H., Browne, M., Donaldson, P., Rose, J., and Rockloff, M. (2016, Jan 27). Understanding gambling related harm: a proposed definition, conceptual framework, and taxonomy of harms. BMC public health, *BioMed Central.* https://doi.org/ 10.1186/s12889-016-2747-0.

Lewins, A., and Silver, C. (2007). Using Software in Qualitative Research: A Step-by-Step Guide. *Sage Publications.* https://doi.org/10.4135/9781473906907.

Liamputtong, P., & Ezzy, D. (2005). Qualitative Research Methods. *Oxford Press,* 270-273. https://doi.org/10.4236/oalib.1107411.

Limbasiya, T., & Das, D. (2019). Energy-efficient and secure communication using batch verification scheme for vehicle users. *Wireless Networks, 25*(7), 4403-4404. https://doi.org/10.1007/s11276-019-02104-5.

Lincoln, S.Y., Guba, E.G. (1985). Naturalistic inquiry. *Sage Publications*, 289-331. https://doi.org/10.1016/0147-1767(85)90062-8.

Lisok, J. (2016). Application of modern technology to improve safety in the automotive industry. *Solid State Phenomena. 246,* 271-274. https://doi.org/10.4028/www.scientific.net/SSP.246.271.

Liu, H., He, J., Wensowitch, K, Rajan, D., Camp, J. (2020 Dec). Architecture and experimental evaluation of context-aware adaptation in vehicular networks. *EURASIP Journal on Wireless Communications and Networking*. https://doi.org/10.1186/s13638-020-01668-7.

Liu, Z., Cai, Y., Wang, H., Chen, L., Gao, H., Jia, Y., and Li, Y. (2021, Feb 24). Robust Target Recognition and Tracking of Self-Driving Cars with Radar and Camera Information Fusion Under Severe Weather Conditions. *IEEE Transactions on Intelligent Transportation System*. https://doi.org/10.1109/TITS.2021.3059674.

Loupis, M. (2014). Embedded systems development tools: A MODUS-oriented market overview. *Business Systems Research, 5*(1), 6-20. https://doi.org/10.2478/bsrj-2014-0001.

Lu, J., Filev, D., Prakah-Asante, K., Tseng, F., Kolmanovsky, I.V. (2009). From vehicle stability control to intelligent personal minder: Real-time vehicle handling limit warning and driver style characterization. *Computational Intelligence in Vehicles and Vehicular Systems*. https://doi.org/10.1109/CIVVS.2009.4938722.

Lu, X., Han, J., Ren, Q., Dai, H, Li, J., and Ou, J. (2018). Network threat detection based on correlation analysis of multi-platform multi-source alert data. *Multimedia Tools and Applications*, 1-15. https://doi.org/10.1007/s11042-018-6689-7.

Lu, Z., Sun, J., and Butts, K. (2011, Oct). Linear Programming SVM-ARM2K With Application in Engine System Identification, *IEEE Transactions on Automation Science and Engineering*, *8*(4), 846-854. https://doi.org/10.1109/TASE.2011.2140105.

Lv, Z. (2020). AI Empowered Communication Systems for Intelligent Transportation Systems. *IEEE transactions on intelligent transportation systems.* https://doi.org/10.1109/TITS.2020.3017183.

Madrigal, F., and Frederic, L. (2020). Robust head pose estimation based on key framesfor human-machine interaction. *EURASIP Journal on Image and Video Processing*. https://doi.org/10.1186/s13640-020-0492-x.

Mallikarjuna Rao, Y., Subramanyam, M.V., and Satya Prasad, K (2018). Cluster-based mobility management algorithms for wireless mesh networks. *International Journal of Communication Systems*, *31*(11), 1. https://doi.org/10.1002/dac.3595.

McDonnell, K., Murphy, F., Sheehan, B., Masello, L., Castignani, G., & Ryan, C. (2021). Regulatory and technical constraints: An overview of the technical possibilities and regulatory limitations of vehicle telematic data. *Sensors,* *21*(10), 3517. https://doi.org/10.3390/s21103517.

McHugh, G. C. (1998). Software process improvement in an automotive electronics organization. *17th DASC. AIAA/IEEE/SAE. Digital Avionics Systems Conference. Proceedings (Cat. No.98CH36267)*, Bellevue, WA, USA, I11/1-I11/6 vol.2, https://doi.org/10.1109/DASC.1998.739862.

Meuleners, M., Quack, D., and Degen, C. (2014). A measurement method for evaluation of car-to-infrastructure radio channels. *The 8th European Conference on Antennas and Propagation (EuCAP 2014)*, The Hague, 1055-1059. https://doi.org/10.1109/EuCAP.2014.6901949.

Miles, D.A. (2017). The One Page Dissertation Proposal Matrix: A Guide for Developing the Dissertation Proposal.

Miles, D.A. and Scott, L. (2017). Workshop: Confessions of a Dissertation Chair Part 1: The Six Mistakes Doctoral Students Make with the Dissertation. *5th Annual 2017 Black Doctoral Network Conference*, Atlanta, GA.

Miles, M., Huberman, M.A., and Saldana, J. (2014). Qualitative Data Analysis: A Methods Sourcebook. *Sage Publications*, 3ed.

Miller C., and Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *2015 Black Hat Conference (USA)*. https://infocondb.org/con/black-hat/black-hat-usa-2015/remote-exploitation-of-an-unaltered-passenger-vehicle.

Milosevic, M., Isic, V., Bjelica, M.Z., and Andjelic, T. (2019). Efficient Implementation of Camera Mirror System Algorithm on Heterogeneous Chip Architectures. *2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin)*, 414-417. https://doi.org/10.1109/ICCE-Berlin47944.2019.8966193.

Mousavinejad, E., Yang, F., Han, Q.L., Ge, X., and Vlacic, L. (2020, Sep). Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning. *IEEE Transactions on*

Intelligent Transportation Systems, *21*(9), 3821-3834. https://doi.org/10.1109/TITS.2019.2934481.

Much, A. (2016). Automotive Security: Challenges, Standards, and Solutions. *Software Quality Professional Journal.* *18*(4), 4-12. https://www.proquest.com/scholarly-journals/automotive-security-challenges-standards/docview/1817024845/se-2.

Nawrath, T., Fischer, D., and Markscheffel, B. (2016). Privacy-sensitive data in connected cars. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Barcelona, 392-393. https://doi.org/10.1109/ICITST.2016.7856736.

Njotini, M.N. (2013). Protecting Critical Databases-Towards a Risk-Based Assessment of Critical Information Infrastructure (CIIS) in South Africa. *Potchefstroom Electronic Law Journal*, *16*(1), 451-481. https://doi.org/10.4314/pelj.v16i1.14.

Nouh, R., Singh, M., & Singh, D. (2021). SafeDrive: Hybrid recommendation system architecture for early safety predication using the internet of vehicles. *Sensors, 21*(11), 3893. https://doi.org/10.3390/s21113893.

Nowell Lorelli, S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis. *International Journal of Qualitative Methods, 16*(1), https://doi.org/10.1177/1609406917733847.

Nuzzo, P., Bajaj, N., Masin, M., Kirov D., Passerone, R., and Sangiovanni-Vicentelli, A.L. (2020, Oct). Optimized Selection of Reliable and Cost-Effective Safety-Critical System Architectures. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *39*(10), 2109-2123. https://doi.org/10.1109/TCAD.2019.2963255.

Oh, S., Bae, C., Cho, J., Lee, S., & Jung, Y. (2021). Command recognition using a binarized convolutional neural network with voice and radar sensors for human-vehicle interaction. *Sensors, 21*(11), 3906. https://doi.org/10.3390/s21113906.

Oh, W. H., Lee, J. H., Kwon, H. G., and Yoon, H. J. (2005) Model-based development of automotive embedded systems: a case of continuously variable transmission (CVT). *11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'05),* Hong Kong, China, 201-204. https://doi.org/10.1109/RTCSA.2005.61.

Park, Y., & Kim, H. (2013, Feb). Collision Control of Periodic Safety Messages with Strict Messaging Frequency Requirements. *IEEE Transactions on Vehicular Technology*, *62*(2), 843-852. https://doi.org/10.1109/TVT.2012.2227070.

Patel, A. M., and Patel, H. R. (2019). Analytical Study of Penetration Testing for Wireless Infrastructure Security. *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, Chennai, India, 131-134. https://doi.org/10.1109/WiSPNET45539.2019.9032741.

Peksa, J. (2020). Prediction framework with Kalman filter algorithm. *Information*, *11*(7), 358. https://doi.org/10.3390/info11070358.

Petit, J., & Mammeri, Z. (2013). Authentication and consensus overhead in vehicular ad hoc networks. *Telecommunication Systems, 52*(4), 2699-2712. https://doi.org/10.1007/s11235-011-9589-y.

Pillmann, J., Sliwa, B., Kastin, C., and Wietfeld, C. (2017). Empirical evaluation of predictive channel-aware transmission for resource-efficient car-to-cloud communication. *2017 IEEE Vehicular Networking Conference (VNC)*, Torino, 235-238. https://doi.org/10.1109/VNC.2017.8275635.

Polit, D.F., Beck, C.T. (2012). Nursing research: Principles and methods. Lippincott Williams & Wilkins.

Qin, X., Bian, Y., Hu, Z., Sun, N., and Hu, M. (2020). Distributed Vehicular Platoon Control Considering Communication Topology Disturbances. *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 1-6. https://doi.org/10.1109/ITSC45102.2020.9294333.

Ramachandran, V. (2021, Feb). Stanford researchers identify four causes for 'Zoom fatigue' and their simple fixes. *Stanford University Press*, https://news.stanford.edu/2021/02/23/four-causes-zoom-fatigue-solutions/

Richards, L., and Morse, J.M. (2007). Readme first for a user's guide to qualitative methods. *Sage Publications*, Thousand Oaks.

Sagor, R. (2017). Chapter 1: What Is Action Research? *ASCD*. https://www.ascd.org/publications/books/100047/chapters/What-Is-Action-Research%C2%A2.aspx>.

Saldana, J. (2015, Dec). The Coding Manual for Qualitative Researchers, 3rd ed, Sage Publications.

Sapsford, R. and Jupp, V. (2006). *Data Collection and Analysis*. New York: Sage Publications.

Sepulcre, M., Gozalvez, J., and Lucas-Estan, M.C. (2019, Sep). Power and Packet Rate Control for Vehicular Networks in Multi-Application Scenarios. *IEEE Transactions on Vehicular Technology*, *68*(9), 9029-9037. https://doi.org/10.1109/TVT.2019.2922539.

Siegel, J.E., Erb, D.C., and Sarma, S.E (2018, Aug). A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, andDevelopment Areas. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2391-2406. https://doi.org/10.1109/TITS.2017.2749459.

Sliwa, B., Falkenberg, R., Liebig, T., Piatkowski, N., and Wietfeld, C. (2020, Aug). Boosting Vehicle-to-Cloud Communication by Machine Learning-Enabled Context Prediction. IEEE Transactions on Intelligent Transportation Systems, *21*(8), 3497-3512. https://doi.org/10.1109/TITS.2019.2930109.

Son, J., Choi, J., and Yoon, H. (2019). New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants, *IEEE Access*, vol. 7, 78379-78390. https://doi.org/10.1109/ACCESS.2019.2922335.

Song, W., Yang, Y., Fu, M., Qiu, F., and Wang, M. (2018, Mar). Real-Time Obstacles Detection and Status Classification for Collision Warning in a Vehicle Active Safety System. *IEEE Transactions on Intelligent Transportation Systems*, *19*(3), 758-773. https://doi.org/10.1109/TITS.2017.2700628.

Sou, S. (2013). Modeling Emergency Messaging for Car Accident over Dichotomized Headway Model in Vehicular Ad-hoc Networks. *IEEE Transactions on Communications*, *61*(2), 802-812. https://doi.org/10.1109/TCOMM.2012.010913.110368.

Spaar, D. (2015). Auto, öffne dich! Sicherheitslücken bei BMWs ConnectedDrive. *C't magazine fur computer tecknik*. http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-sConnectedDrive-2540957.html.

Spencer, L., Ritchie, J., Lewis, J., Dillon, L. (2003). Quality in qualitative evaluation: a framework for assessing research evidence. *National Centre for Social Research*, https://www.heacademy.ac.uk/system/files/166_policy_hub_a_quality_framework.pdf

Srihari, K. (2021, Mar 26). Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT Based Bat Agents for Traffic Management. *Electronics (Basel)*, *10*(7), 785. https://doi.org/10.33390/electronics10070785.

Srinivasan, R., McFarlane, D., Parlikad, A., and Catton, P. (2013). Condition monitoring for infrastructure assets: Building the business case. *IET IAM Asset Management Conference 2013*, 1-15. https://doi.org/10.1049/cp.2013.1944.

Stocklein, J., Geiger, C., Paelke. V., and Pogscheba, P. (2009). Poster: MVCE - a design pattern to guide the development of next-generation user interfaces. *2009 IEEE Symposium on 3D User Interfaces*, Lafayette, LA, 153-154. https://doi.org/10.1109/3DUI.2009.4811232.

Sugumar, R., Rengarajan, A., & Jayakumar, C. (2018). Trust-based authentication technique for cluster-based vehicular ad hoc networks (VANET). *Wireless Networks*, *24*(2), 373-382. https://doi.org/10.1007/s11276-016-1336-6.

Sun, T., Qiao, L., Liao, Q., and Li, D. (2020, Nov 25). Novel Convergence Results of Adaptive Stochastic Gradient Descents. *IEEE Transactions on Image Processing*, 30, 1044-1056. https://doi.org/10.1109/TIP.2020.3038535.

Taghvaeeyan, S., and Rajamani, R. (2012, Dec). The Development of Vehicle Position Estimation Algorithms Based on the Use of AMR Sensors. *IEEE Transactions on Intelligent Transportation Systems*, *13(*4), 1845-1854. https://doi.org/10.1109/TITS.2012.2208189.

Taş, Ö.Ş., Hörmann, S., Schäufele, B., and Kuhnt, F. (2017). Automated vehicle system architecture with performance assessment. *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, 2017, 1-8. https://doi.org/10.1109/ITSC.2017.8317862.

Temponi, C. (2005). Continuous improvement framework: Implications for academia. *Quality Assurance in Education, 13*(1), 17-36. https://dx.doi.org/10.1108/09684880510578632.

Terrell, S. R., PhD. (2012). Mixed-methods research methodologies. *The Qualitative Report, 17*(1), 254-280. https://www.proquest.com/scholarly-journals/mixed-methods-research-methodologies/docview/920733426/se-2.

Thimmaraju, K. (2021). Preacher: Network Policy Checker for Adversarial Environments. *IEEE/ACM Transactions on Networking*, 1-14. https://doi.org/10.1109/TNET.2021.3078143.

Tien, C., Tsai, T., Chen, I., and Kuo, S. (2018). UFO - Hidden Backdoor Discovery and Security Verification in IoT Device Firmware. *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, 18-23. https://doi.org/10.1109/ISSREW.2018.00-37.

Tu, L., Wang, S., Zhang, D., Zhang, F., and He, T. (2021, Jan). ViFi-MobiScanner: Observe Human Mobility via Vehicular Internet Service, *IEEE Transactions on Intelligent Transportation Systems*, *22*(1), 280-292. https://doi.org/10.1109/TITS.2019.2956744.

Turner, P., & Turner, S. (2009). Triangulation in practice. *Virtual Reality, 13*(3), 171-181. https://doi.org/10.1007/s10055-009-0117-2.

Urban, D., and Caplier, A. (2021). Time- and resource-efficient time-to-collision forecasting for indoor pedestrian obstacles avoidance. *Journal of Imaging*, *7*(4), 61. https://doi.org/10.3390/jimaging7040061.

Wang, G., Qiao, J., Liu, C., and Shen, Z. (2021, May 7). How Deep is Deep Enough for Deep Belief Network for Approximating Model Predictive Control Law. *IEEE Transactions on Automation Science and Engineering.* 1-12. https://doi.org/10.1109/TASE.2021.3074984.

Wang, X., Han, S., Yang, L., Yao, T., and Li, L. (2020, May). Parallel Internet of Vehicles: ACP-Based System Architecture and Behavioral Modeling. *IEEE Internet of Things Journal*, *7*(5), 3735-3746. https://doi.org/10.1109/JIOT.2020.2969693.

Widhiasi, A., Mohanan, V., Pasha, M. F., and Budiarto, R. (2010). Vertical Handover Scheme for Car-to-Car Communication Based on IEEE 802.21 Standard. *2010 Second International Conference on Computer Engineering and Applications*, Bali Island, 143-147. https://doi.org/10.1109/ICCEA.2010.36.

Wright, A. (2011). Hacking Cars. *Communications of the ACM, 54*(11), 18. https://cacm.acm.org/magazines/2011/11/138210-hacking-cars/fulltext

Wu, T., Li, J., Qin, X. (2021). Braking performance oriented multi-objective optimal design of electro-mechanical brake parameters. *PLoS ONE*, *16*(5). https://doi.org/10.1371/journal.pone.0251714.

Wu, W., Liu, R., Yang, Q., Shan, H., and Quek, T.Q.S. (2021, Mar 22). Learning-based Robust Resource Allocation for Ultra-Reliable V2X Communications. *IEEE Transactions on Wireless Communications,* *20*(8), 5199-5211. https://doi.org/10.1109/TWC.2021.3065996.

Xiao,S.,Ge,X.,Han,Q.L.,andZhang,Y.(2021,May25).SecureDistributedAdaptivePlatooning Control of Automated Vehicles Over Vehicular Ad-Hoc Networks Under Denial-of- Service Attacks. *IEEE Transactions on Cybernetics*, 1-13. https://doi.org/10.1109/TCYB.2021.3074318.

Xiong, H., Tan, Z., Zhang, R., and He, S. (2020, Apr 4). A New Dual Axle Drive Optimization Control Strategy for Electric Vehicles Using Vehicle-to-Infrastructure Communications. *IEEE Transactions on Industrial Informatics*, 2574-2582. https://doi.org/10.1109/TII.2019.2944850.

Xu, Q., Mak, T., Ko, J., and Sengupta, R. (2004, Oct). Vehicle-to-vehicle safety messaging in DSRC. *Proceedings of the 1st ACM International workshop on Vehicular ad hoc networks*, 19-28. https://doi.org/10.1145/1023875.1023879.

Yao,Y.,Fu,Q.,Yang,W.,Wang,Y.,&Sheng,C.(2018).Anepidemicmodelofcomputerworms with time delay and variable infection rate. *Security and Communication Networks*, 11. https://doi.org/10.1155/2018/9756982.

Yeh, E. R., Choi, J., Prelcic, N.G., Bhat, C.R., Heath, Jr, R.W. (2017). Security in automotive radar and vehicular networks. *Microwave Journal, 60*(5), 148-164. https://proquest.com/docview/1899810395.

Yin, J.L., Chen, B.H., Lai, K.H., and Li, Y. (2018, Jun 15). Automatic Dangerous Driving Intensity Analysis for Advanced Driver Assistance Systems from Multimodal Driving Signals. *IEEE Sensors Journal*, *18*(12), 4785-4794. https://doi.org/10.1109/JSEN.2017.2765315.

Yoo, S., Song, S., Kim, K., Park, C., & Gong, J. (2012). Multi-function unit for LED lighting. *2012 International SoC Design Conference (ISOCC),* 447-450. https://doi.org/10.1109/isocc.2012.6406892.

Yu, D., Zou, Z., Chen, S., Tao, Y., Tian, B., LV, W., and Cheng, X. (2021). Decentralized Parallel SGD with Privacy Preservation in Vehicular Networks. *IEEE Transactions on Vehicular Technology,* 5211-5220. http://doi.org/10.1109/TVT.2021.3064877.

Yu, J., and Luo, F. (2020). A systematic approach for cybersecurity design of in-vehicle network systems with trade-off considerations. *Security and Communication Networks*. https://doi.org/10.1155/2020/7169720.

Yu, P., Ni, W., Yu, G., Zhang, H., Liu, R.P. and Wen, Q. (2021). Efficient anonymous data authentication for vehicular ad hoc networks. *Security and Communication Networks*. https://doi.org/10.1155/2021/6638453.

Zaidi, K., Milojevic, M.B., Rakocevic, V., Nallanathan, A., and Rajarajan, M. (2016).Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue NodeDetection. *IEEE*

Transactions on Vehicular Technology, *65*(8), 6703-6714. https://doi.org/10.1109/TVT.2015.2480244.

Zeadally, S., Guerrero, J., and Contreras, J. (2020). A tutorial survey on vehicle-to-vehicle communications. *Telecommunication Systems*, 469-489. https://doi.org/10.1007/s11235-019-00639-8.

Zhang, Y.J., Du, F., Wang, J., Ke, L.S., and Wang, M. (2020). A safety collision avoidance algorithm based on comprehensive characteristics. *Complexity,* 1-13. https://doi.org/10.1155/2020/1616420.

Zhang, J., and Li, C. (2020, Jul). Adversarial Examples: Opportunities and Challenges. *IEEE Transactions on Neural Networks and Learning Systems*, *31*(7), 2578-2593. https://doi.org/10.1109/TNNLS.2019.2933524.

Appendix A: Informed Consent

Title of Study: *Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers*
Principal Investigator Name: Hector Cruz Platon
CTU Email Address:xxxxxxx@student.ctuonline.edu
Contact Phone Number: (xxx)xxx-xxxx

Purpose of the Study

You are invited to participate in a research study. The purpose of this study is to explore vehicle security improvement frameworks (VSIF) in the safety messaging system to protect against externalhackers.

InclusionCriteria

You are invited to participate in the study because you meet the following inclusion criteria:

- Knowledge within Vehicle Ad HocNetworks
- Skills within Vehicle Ad HocNetworks
- Abilities within Vehicle Ad HocNetworks

This form may help you determine whether or not you desire to participate in this study.

Study Activities and Duration

If you volunteer to participate in this study, you will be asked to do the following:

- Answerquestions
- Ratequestions
- Describe and provide improvementmethods_

Benefits to You orOthers

There is likely no direct benefit to you for study participation. However, the overall benefits of the study may include better understanding how to protect in-vehicular systems, embedded systems, particularly safety messaging system to external hackers. If you choose to review the interview, anonymized results will be sent over through the results/findings.

Risks or Discomfort

There is some level of risk or discomfort involved in all research studies. This study is estimated to involve no more than minimal risk. A good example of risk is feeling uncomfortable sharing the auto organization’s information that are private and protected by copyright, or by non-disclosure agreements, or accetable use agreements of technologies.

Incentives to Participation

There will be no financial cost to you to participate in this study. For your time, I will be providing an incentive of $20 visa gift card.

Voluntary Participation

Your participation in this study is voluntary. You may choose not to participate in this study and may withdraw at any time or suspend responses at any time without penalty or consequence. You are also encouraged to ask questions about this study at the any time.

Privacy and Confidentiality

All participation will be protected rigorously for confidentiality. Virtual In-person interviews will be conducted with qualitative codes and labels to anonymize the participants identity, anddata interactions will be encrypted from end-to-end. Labels resembling ‘p01’, ‘c01’, or ‘a01’ willbe leveraged to anonymize participant identity, yet give an indication into the participant’s role or job function. These same labels will also be used on background surveys, and all collected data will be predicated by the assignment of a participant code before any interview or survey activities are performed.

If you have any questions or concerns about the study, you may contact the Principal Investigator noted above. [Dr. Hughes, Kelly, Supervisor, KHughes@coloradotech.edu, 719-270-0905]. For additional questions, you may contact the CTU IRB at CTUIRB@coloradotech.edu or visit IRB resources athttps://careered.libguides.com/ctu/doctoral_students/irb

Participant Consent

I have read the above information and agree to participate in this study. My signature below certifies I am at least 18 years of age and agree to study participation. A copy of this form has been given to me.

______________________________	________________
SignatureofParticipant	Date

____

Participant Name (Please Print)

Appendix B: Demographic Questions

Title of Study: *Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers*
Principal Investigator Name: Hector Cruz Platon
CTU Email Address:xxxxxxx@student.ctuonline.edu
Contact Phone Number: (xxx)xxx-xxxx

Vehicle Security Improvement Framework (VSIF) Background Data
Greetings highly esteemed participants! The goal of the interview is to capture data relating to the exploration of the vehicle security improvement framework (VSIF) due to the vulnerability of safety messaging system to external hackers.

*** All data that will be provided are protected within the Informed Consent that accompanies this questionnaire***

1. Please select job title that best fits your currentrole?
   a. Chief Information Officer
   b. Chief TechnologyOfficer
   c. Chief Information SecurityOfficer
   d. SystemsArchitect
   e. SecurityArchitect
   f. SystemsManager
   g. SecurityManager
   h. ConfigurationManager
   i. Hardware Engineer
   j. Software Engineer
   k. Security Engineer
   l. Security Analyst
2. What best describes your coremission?
   a. Automotive
   b. Manufacturing
   c. Supply Chain
   d. Engineering
   e. Communications, Computer Networks, CyberSecurity
3. How big is yourorganization?
   a.0-100
   b. 100-500
   c. 500-1,000

d. 1,000-10,000
e. 10,000-50,000
f. 50,000-100,000
g. 100,000 or greater

4. On a scale of 1-10, how would you describe your expertise in Vehicle ad hocNetworks (VANETS) in regard to security improvement of safety messagingsystem?
   0 = No experience
   1 = has general understanding of the vehicle ad hoc network
   2 = Analyst in the vehicle ad hoc network and Internet of Vehicle area
   3 = Engineer in the vehicle ad hoc network and Internet of Vehiclearea
   4 = Project Manager in the vehicle ad hoc network and Internet of Vehicle area
   5 = Program Manager in the vehicle ad hoc network and Internet of Vehiclearea
   6 = Consultant in the vehicle ad hoc network and Internet of Vehiclearea
   7 = Executive in the vehicle ad hoc network and Internet of Vehicle are
5. How long have you been working with Vehicle ad hocnetworks?
   a. 1-5years
   b. 5-10years
   c. 10-15years
   d. 15-20years
   e. 20-25years
   f. 25-30years
6. What is your highest degree?
   a. Associates: A.S., A.A.
   b. Bachelors: B.S., B.A.,B.E.,
   c. Masters: M.S., M.A., M.E.,M.B.A.
   d. Doctoral: Ph.D, D.Eng., D.Sc., Ed.D., D.C.S.,D.A.
7. What is your field of study?
   a. Science
   b. Technology
   c. Engineering
   d. Mathematics

Appendix C: Interview Questions

Title of Study: *Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers*
Principal Investigator Name: Hector Cruz Platon
CTU Email Address:xxxxxxx@student.ctuonline.edu
Contact Phone Number: (xxx)xxx-xxxx

Greetings highly esteemed participants! The goal of the interview is to capture data relating to the exploration of the vehicle security improvement framework (VSIF) due to the vulnerability of safety messaging system to external hackers.

*** All data that will be provided are protected within the Informed Consent that accompanies this questionnaire***

1) Briefly describe your role (automotive, manufacturing, supply chain,engineering, cybersecurity, network) as it relates to automotive manufacturer and security assessment (ifappropriate).
   a. *Probe Question*: How are you involved in the teaching, learning, and security assessmenthere?
   b. *Probe Question*: How did you getinvolved?
2) What is the strategy at this institution for improving security learning, and security assessment to prevent undesirable external attacks tonetwork?
   a. *Probe Question*: Is itworking?
   b. *Probe Question*: Why or whynot?
3) What is the biggest misconception about vehicle security that is apparent intoday's automotive manufacturing?
   a. *Probe Question*: Why do you thinkso?
4) What are some of the major challenges your department faces in attempting tochange security learning, and security assessment practices in safety messagingsystems?
5) What element are you willing to give up for a good connected network onvehicles?
6) How far are you willing to go as a cybersecurity team to be protected againsthackers?
7) What are the secure standards you use for vehicle ad hocnetworks?
8) What are the possible vehicle security improvement framework in the safety messaging system to protect against externalhackers?
   a. *Probe Question*: How can barriers be overcome for safety messagingsystem?
   b. *Probe Question*: How can opportunities be maximized for safety messagingsystem?
9) What kind of resistance did you and your colleagues get during security improvement meetings?
   a. *Probe Question*: How often do you get this as aresult?

10) To what extent are security improvement-related activities evaluated at your institution and yourdepartment?
    a. *Probe Question*: How is security improvementrewarded?

Appendix D: Interview Protocol

Title of Study: *Exploring Vehicle Security Improvement Framework in the Safety Messaging System to Protect Against External Hackers*
Principal Investigator Name: Hector Cruz Platon
CTU Email Address:xxxxxxx@student.ctuonline.edu
Contact Phone Number: (xxx)xxx-xxxx

To facilitate our notetaking, we would like to record our conversations today. Please sign the release form. For your information, only principal investigator on the project will be privy to the recordings which will be eventually destroyed after they are transcribed. In addition, you must sign a form devised to meet our human subject requirements. Essentially, this document stats that: (1) all information will be held confidential, (2) your participation is voluntary and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm. Thank you for your agreeing to participate.

We have planned this interview to be given at least 50 minutes time frame for the semi-structured interview. During this time, we have several questions that we would like to cover. If time begins to run short, it may be necessary to interrupt you in order to push ahead and complete this line of questioning.

You have been selected to speak with us today because you have been identified as someone as a Subject Matter Expert (SME) who has a great deal to share about their individual knowledge, skills and abilities on Vehicle ad hoc networks, embedded system, and protection of information assets in motion and at rest. The research project as a whole focus on the exploration of vehicle security improvement framework, with particular interest in understanding how the conversation today could be formulate improvement in critical systems such as safety messaging system to its desires to protect against external hackers effectively.

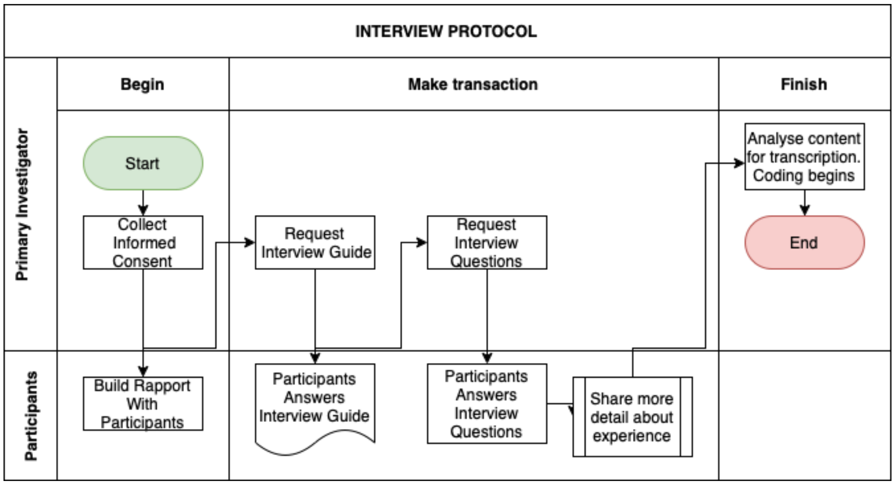

INTERVIEW PROTOCOL
Begin
Make transaction
Finish
Primary Investigator
Participants
Start
Collect Informed Consent
Request Interview Guide
Request Interview Questions
Analyse content for transcription. Coding begins
End
Build Rapport With Participants
Participants Answers Interview Guide
Participants Answers Interview Questions
Share more detail about experience

Figure 4. Interview Protocol

Each interview will include the following process: (a) Collect Informed Consent; (b) build rapport with participants; (c) request interview guide; (d) participants answers interview guide; (e) request interview questions; (f) participants answers interview questions; (g) share more detail about experience (probe), (h) thank the participants for their time and provide the$20 gift card, and (h) analyze content for transcription and begincoding.